THE UNIVERSITY
of EDINBURGH

A PUBLIC INTEREST APPROACH TO DATA PROTECTION LAW:

The meaning, value and utility of the public interest for research uses of data

LESLIE ANNE STEVENS BA JD LLM

The University of Edinburgh
Ph.D. in Law
2017

Abstract

Due to legal uncertainty surrounding the application of key provisions of European and UK data protection law, the public interest in protecting individuals' informational privacy is routinely neglected, as are the public interests in certain uses of data. Consent or anonymisation are often treated as the paradigmatic example of compliance with data protection law, even though both are unable to attend to the full range of rights and interests at stake in data processing. Currently, where data processing may serve a realisable public interest, and consent or anonymisation are impracticable (if not impossible to obtain) the public interest conditions to processing are the rational alternative justifications for processing. However, the public interest conditions are poorly defined in the legislation, and misunderstood and neglected in practice. This thesis offers a much-needed alternative to the predominant consent-or-anonymise paradigm by providing a new understanding of the public interest concept in data protection law and to suggest a new approach to deploying the concept in a way that is consistent with the protective and facilitative aims of the legislation.

Through undertaking legislative analysis new insight is provided on the purpose of the public interest conditions in data protection law, revealing critical gaps in understanding. By engaging with public interest theory and discovering the conceptual contours of the public interest, these gaps are addressed. Combined with the insight obtained from the legislative history, we can determine the reasonable range of circumstances and types of processing where it may be justifiable to use personal data based on the public interest. On this basis, and to develop a new approach for deploying the concept, other legal uses of the public interest are examined. The lessons learned suggest legislative and procedural elements that are critical to successful deployment of the public interest concept in data protection. The thesis concludes with the identification of key components to allow a clearer understanding of the public interest in this field. Further, these insights enable recommendations to be made, to reform the law, procedure and guidance. In doing so, the concept of the public interest can be confidently deployed in line with the aims of data protection law, to both protect and facilitate the use of personal data.

Lay Summary

Due to legal uncertainty surrounding the application of key provisions of European and UK data protection law, the public interest in protecting individuals' informational privacy is routinely neglected, as are the public interests in certain uses of data. Consent or anonymisation are often treated as the definitive example of compliance with data protection law, even though both are unable to fully protect the rights and interests at stake when personal data are used. Currently, where the use of data may serve a realisable public interest, such as for research, and consent or anonymisation are impracticable (if not impossible to obtain) the public interest conditions are the rational legal justifications for processing. However, the public interest conditions are poorly defined in the legislation, and misunderstood and neglected in practice. This thesis offers a much-needed alternative to the predominant mode of compliance through consent or anonymisation by providing a new understanding of the public interest concept in data protection law.

By analysing current data protection legislation, new insight is provided on the purpose of the public interest conditions, revealing critical gaps in understanding how the public interest in a use of data can be assessed. By looking to public interest theory and discovering the conceptual contours of the public interest, these gaps are addressed. Combined with the insight obtained from the legislative analysis, we can determine the range of circumstances where it may be justifiable to use personal data based on the public interest. To understand what is practically required to deploy the concept in law, other legal uses of the public interest are examined. The lessons learned suggest legislative and procedural elements that are critical to successful deployment of the public interest concept in data protection. The thesis concludes with the identification of key components to allow a clearer understanding of the public interest in this field. Further, these insights enable recommendations to be made, to reform the law, procedure and guidance. In doing so, the concept of the public interest can be confidently deployed in line with the aims of data protection law, to both protect and facilitate the use of personal data.

Declaration

This is to certify that the work contained within has been composed by me and is entirely my own work. No part of this thesis has been submitted for any other degree or professional qualification.

Signed _____

Contents

Abbreviations

Term	Abbreviation
Administrative Data Research Centre Scotland	ADRC-S
Administrative Data Research Network	ADRN
Court of Justice of the European Union	CJEU
Data Protection Act 1998 (UK)	DPA 1998
Data Protection Directive 95/46/EC	DPD
Data Protection (Processing of Sensitive Personal Data) Order 2000 (UK)	DPPSPD 2000
European Convention on Human Rights	ECHR
European Court of Human Rights	ECtHR
General Data Protection Regulation	GDPR
Information Commissioner's Office	ICO
Scottish Information Commissioner	SIC
United Kingdom Supreme Court	UKSC

Chapter 1 Addressing the Public Interest Gap in Data Protection Law and Practice

1. Introduction

This thesis is concerned with the use of the public interest concept in data protection law. Under what conditions can an individual or organisation justify the processing[1] of personal data[2] based on the public interest? How is this public interest 'claim' to be assessed within data protection law? My focus is on the use of the public interest within the legal conditions for processing personal data in UK data protection legislation and practice. I consider the lack of a coherent understanding of 1) what the concept means; and 2) how it should be deployed by those who process personal data ('data controllers'[3]) and those who must review (when legally necessary) these decisions, including the UK's data protection supervisory authority – the Information Commissioner's Office ('ICO')[4] – and the courts. My contribution lies in offering a

---

[1] All websites in this thesis were accessed on 22 October 2017.
In data protection law, the use of personal data is regulated if it involves any activity regarded as 'processing'. This is defined under the Data Protection Directive 95/46/EC ('DPD') Art 2(b) as: '…any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction'. The UK's Data Protection Act 1998 ('DPA 1998') s 1(1) similarly defines processing as: 'in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including— (a) organisation, adaptation or alteration of the information or data, (b) retrieval, consultation or use of the information or data, (c) disclosure of the information or data by transmission, dissemination or otherwise making available, or (d) alignment, combination, blocking, erasure or destruction of the information or data'.
[2] Understood within this thesis per the legal definition provided in the DPA 1998 s 1(1): '…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, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual'.
[3] A term defined under the DPA 1998 s 1(1): '…a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.'
[4] The UK Information Commissioner's Office ('ICO') (and Information Commissioner) are obligated 'to promote the following of good practice by data controllers and, in particular, so to perform his

new understanding and approach to the public interest concept in data protection law which is capable of attending to the public interests both in protecting informational privacy and in the undertaking of publicly beneficial uses of data.

2. The Legal Context

Over the last five years, European data protection law has been subject to an intensive reform effort, with the final text of the new General Data Protection Regulation ('GDPR')[5] approved and set for implementation by Member States in May 2018.[6] Since the enactment of the current Data Protection Directive 95/46/EC ('DPD')[7], the growing use of personal data has raised significant practical, legal and ethical concerns. The DPD (effected by Member States' implementing legislation) was to provide legal certainty and a level regulatory playing field for data controllers operating within the EU, which would simultaneously afford consistent protection to EU citizens.[8] It is important to understand from the outset that the purpose of the DPD is twofold: to *protect* individuals' rights and other interests in their data (most notably their informational privacy[9]) *and* to *facilitate* the free flow of personal data within the EU.[10] It is also important to distinguish between the protections offered under data protection law – discrete rights related to the use of an individual's personal data – which are separate from (although potentially overlapping with) that same person's right to respect for private and family life under both Article 7 of the Charter of Fundamental Rights of the European Union ('CFR') and Article 8 of the European

functions under this Act as to promote the observance of the requirements of this Act by data controllers.' DPA 1998, s 51.

[5] 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) ('GDPR').

[6] 'Reform of EU Data Protection Rules' <http://ec.europa.eu/justice/data-protection/reform/index_en.htm>.

[7] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281 'Data Protection Directive' ('DPD').

[8] DPD, Recitals 7-8.

[9] As distinguished from a broader right to privacy as, for example, enshrined in Article 8 of the European Convention on Human Rights ('ECHR').

[10] For example, DPD, Recital 3.

Convention on Human Rights ('ECHR').[11] Anita Allen helpfully distinguishes between four types of privacy:

> (1) Informational privacy concerns access to personal information; (2) physical privacy concerns about access to persons and personal spaces; (3) decisional privacy concerns about governmental and other third-party interference with personal choices; and (4) proprietary privacy concerns about the appropriation and ownership of interests in human personality.[12]

Of these, potentially the most relevant to this thesis is *informational privacy*, although it is acknowledged that uses of *information* (and specifically personal data) may impact upon the other types of privacy put forward by Allen. Consider the 2009 firing of 'Lindsay' for berating her boss on Facebook while neglecting to remember he was one of her friends on the website;[13] or the dire consequences for a family home and community when a 16-year-old's birthday party invitation went viral;[14] and finally the unfortunate outcome from bragging about your vacation when unsuspecting burglars are prowling your social media profile.[15] It is unnecessary for the purposes of this thesis to engage in a broader debate on the differences between rights to private and family life as enshrined in human rights law, versus the rights and interests protected within data protection (or as to 'personal data' under Article 8 of the CFR). Nevertheless, I would argue that the aims of human rights law vis-à-vis privacy are at least partially different to the aims of data protection legislation[16]. Whereas the former is charged

---

[11] The Treaty of Lisbon 2009 gives direct effect to the CFR which has its own discrete right to data protection (in its Article 8) and to privacy in Article 9. Thus, the CFR is the primary human rights law instrument that governs secondary EU law such as the DPD, forthcoming GDPR and any Member State's implementing legislation on data protection. Charter of Fundamental Rights of the European Union 2012/C 326/02, Art 7-8 ('CFR'). See discussion on distinguishing between rights to privacy and data protection law: Gillian Black and Leslie Stevens, 'Enhancing Data Protection and Data Processing in the Public Sector: The Critical Role of Proportionality and the Public Interest' (2013) 10 SCRIPTed 1, 108–109.

[12] Anita Allen, 'Genetic Privacy: Emerging Concepts and Values', *Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era* (YUP 1997) 33.

[13] Cathal Kelly, 'Facebook Firing after "Friend" Boss Ripped' <http://cybersmokeblog.blogspot.co.uk/2009/08/facebook-firing-after-friend-boss.html>.

[14] NBC News Staff and Wire Reports, 'Thousands Descend on Tiny Dutch Town after Facebook Invitation Goes Viral' (*NBC News*, 22 September 2012) <http://worldnews.nbcnews.com/_news/2012/09/22/14028638-thousands-descend-on-tiny-dutch-town-after-facebook-invitation-goes-viral?lite>.

[15] Casey Johnston, 'Post Smug Vacation Statuses on Facebook, Get Your House Burgled' (*Ars Technica*, 2012) <http://arstechnica.com/tech-policy/2012/06/post-smug-vacation-statuses-on-facebook-get-your-house-burgled/>.

[16] As argued throughout this thesis that the purpose of data protection *is* twofold and not solely about protecting informational privacy. For example, consider Recital 3 of the DPD. Thus, statements such

with protecting the private 'life' of an individual, the latter is concerned with the protection of privacy to the extent that it relates to personal data, whereby data protection law is equally focused on facilitating uses of data.

A fundamental protection for individuals under data protection law is that data controllers must demonstrate their use of personal data is *lawful*.[17] To be lawful, the processing of personal data must satisfy certain legal 'conditions'.[18] As stated above, I primarily concerned with the implementation of the *public interest conditions* for processing, and here I look in particular at the UK's implementation of the DPD in the DPA 1998.

In the UK, data controllers must *independently* determine what their legal basis is for processing personal data i.e. which legal condition for processing they will rely upon. Data controllers may establish their legal basis either by obtaining an individual's consent or by demonstrating their use of personal data is necessary for a particular purpose (e.g. to carry out a contract).[19] This determination is not reviewed unless the ICO later intervenes or there are subsequent adjudicative proceedings. In the DPA 1998, the public interest concept is found within the legal conditions justifying the processing of both 'ordinary'[20] and 'sensitive'[21] personal data, but the term itself is not

---

as by Buxton LJ in the Court of Appeal are simply incorrect (i.e. that 'It is not easy to extract from this Directive any purpose other than the protection of privacy.') *Johnson v Medical Defence Union* (No 1) [2007] EWCA Civ 262 [16].

[17] DPD, Art 6(1)(a); DPA 1998, Sch 1, para 1.

[18] Throughout the thesis, I refer to these as the 'conditions for processing' personal data or 'the public interest conditions' for short. DPD, Recital 30; DPA 1998, Sch 1, paras 1(a)-(b).

[19] DPD, Art 7(a), (b).

[20] I use the term 'ordinary' where necessary to clearly distinguish between 'personal' and 'sensitive' personal data, which are subject to differing legal provisions within data protection legislation. I use the term 'personal data', on its own, to refer to both personal *and* sensitive personal data. For example, in the sentence on page 7 above ('My focus is on the use of the public interest within the legal conditions for processing personal data in UK data protection legislation and practice.') Here I am referencing *both* categories of data.

[21] In both the DPD and DPA 1998 certain types of personal data – called 'special categories of data' under the DPD and 'sensitive data' under the DPA 1998 – require data controllers to satisfy additional legal justifications to process. Under the DPD Art 8(1), special categories of data are defined as: 'personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life'. Under the DPA 1998 s 2, sensitive data are defined as '…personal data consisting of information as to— (a) the racial or ethnic origin of the data subject, (b) his political opinions, (c) his religious beliefs or other beliefs of a similar nature, (d) whether he is a member of a trade union (within the meaning of the M1Trade Union and Labour Relations (Consolidation) Act 1992), (e) his physical or mental health or condition,

defined. Per Schedule 2 paragraph 5(d), the processing of *ordinary* personal data is justified if '[the] processing is necessary…for the exercise of any other functions of a public nature exercised in the public interest by any person.' As to the legal conditions applicable to the processing of *sensitive* personal data,[22] there is no blanket justification for processing based on the public interest. Instead, specific legal conditions were later added by the Data Protection (Processing of Sensitive Personal Data) Order 2000 ('DPPSPD 2000') to justify particular types of processing, such as for research purposes, based on it being in the 'substantial public interest'.[23] Even though the public interest is used as a final point of consideration when applying these legal conditions, the concept is undefined, as are other operative terms (e.g. 'necessary' and 'public nature').[24] The public interest conditions have *not* been the subject of comprehensive guidance from the relevant supervisory authorities at the EU[25] or UK level[26], and have

---

(f) his sexual life, (g) the commission or alleged commission by him of any offence, or (h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings'. Thus, the DPA 1998's definition of sensitive data is more expansive, by explicitly including data on mental health, the commission or alleged commission of a crime/offence and on any proceeding regarding that offence.

[22] In DPA 1998, Sch 3.

[23] These were added to Sch 3 by the DPPSPD 2000. For example, under the DPPSPD 2000 Sch, para 9, the processing of sensitive personal data for research is justified if: 'the processing…(a) is in the substantial public interest; (b) is necessary for research purposes (which expression shall have the same meaning as in section 33 of the Act); (c) does not support measures or decisions with respect to any particular data subject otherwise than with the explicit consent of that data subject; and (d) does not cause, nor is likely to cause, substantial damage or substantial distress to the data subject or any other person.'

[24] Considered in Chapter 3 Section 3.

[25] In reference to the Article 29 Working Party which is 'composed of representatives of the national data protection authorities (DPA), the EDPS and the European Commission. It is a very important platform for cooperation, and its main tasks are to: Provide expert advice from the national level to the European Commission on data protection matters. Promote the uniform application of Directive 95/46 in all Member States of the EU, as well as in Norway, Liechtenstein and Iceland; Advise the Commission on any European Community law (so called first pillar), that affects the right to protection of personal data.' The public interest conditions reflected in Article 7(e) and Article 8(4) of the DPD are briefly commented on by the Article 29 Working Party in early guidance on the reuse of data by public authorities. In this guidance, they merely state that the applicability of the public interest conditions is to be determined by the public authority in the first instance and that this '…consequently leaves a certain margin of appreciation.' No further direction is provided as to how this public interest in processing should be assessed. Article 29 Data Protection Working Party, 'Opinion 7/2003 on the Re-Use of Public Sector Information and the Protection of Personal Data: Striking the Balance' (2003) 5 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2003/wp83_en.pdf>; 'Article 29 Working Party' (*European Data Protection Supervisor*) <https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/Art29>.

[26] In reference to the ICO. The public interest conditions, as to either ordinary or sensitive personal data, are not addressed in the ICO's most recent data protection guidance. ICO, 'The Guide to Data Protection' (2016) <https://ico.org.uk/media/for-organisations/guide-to-data-protection-2-4.pdf>.

received relatively little critical attention within legal practice[27] or academia[28]. Under what circumstances *can* an individual or organisation (whether public, private or third-sector) lawfully process personal data because it is deemed to be 'in the public interest'? Without a definition in the law or subsequent guidance, how can the 'public interest' in the processing of personal data be legitimately assessed? In other words, how can we prevent the use of the public interest, as a legal justification for processing, from becoming nothing more than empty rhetoric, meaning only what the individual making the claim wishes it to mean?

3. The Problem: The Uncertain Role and Scope of the Public Interest Conditions for Processing Personal Data

Since the enactment of the DPA 1998, a persistent problem for data controllers has been the uncertainty surrounding the legality of certain uses of personal data: it has been unclear what legal grounds they can (or should) rely upon to demonstrate the lawfulness of processing (e.g. such as through consent). Are the several alternative legal justifications in the conditions for processing 'equal' or is there an implicit hierarchy amongst these routes to legality?

Neither the DPD nor DPA 1998 contains explicit or implicit preferences for any particular legal avenue to legitimise the use of personal data.[29] However, the ambiguity over key terminology within the various conditions has led to pervasive legal uncertainty in practice.[30] This legal uncertainty has proven inhibitive to the use of

---

[27] Considered by UK data protection practitioner, Rosemary Jay, to merely be a 'mopping-up' provision that is likely to have its interpretation challenged through the courts by way of judicial review. Rosemary Jay, *Data Protection Law & Practice* (4th edn, Sweet & Maxwell 2012) 266.

[28] This lack of critical attention is discussed in Chapter 2 and Chapter 4, Section 2. Some notable exceptions are: Aileen McHarg, 'Reconciling Human Rights and the Public Interest: Conceptual Problems and Doctrinal Uncertainty in the Jurisprudence of the European Court of Human Rights' (1999) 62 Modern Law Review 671, 671, 674; Graeme Laurie, *Genetic Privacy: A Challenge to Medico-Legal Norms* (CUP 2002) 279–298; David Townend, 'Overriding Data Subjects' Rights in the Public Interest' in Deryck Beyleveld and others (eds), *The Data Protection Directive and Medical Research Across Europe* (Ashgate 2004); Deryck Beyleveld, 'Data Protection and Genetics: Medical Research and the Public Good' (2007) 18 King's Law Journal 275; Mark Taylor, *Genetic Data and the Law: A Critical Perspective on Privacy Protection* (CUP 2012); Black and Stevens (n 11).

[29] DPD, Arts 7-8; DPA 1998, Sch 2 and Sch 3.

[30] For example, the meaning of the 'public interest' in Art 7(e) and 'legitimate interests' in Art 7(f).

personal data for research, the processing context I will make specific reference to throughout this thesis.[31] The application of data protection law to research in the social sciences and humanities is of particular interest in light of the biomedical preoccupation of much of the literature.[32]

The use of personal data for research is not 'lawful' in itself.[33] This means that any use of personal data for research must be justified on one of the legal conditions for processing, such as consent.[34] Furthermore where research requires the use of data originally collected for purposes *other than* research (e.g. reuse of data originally collected by a public body), the data controller must ensure that the reuse is compatible.[35] The legal uncertainty surrounding research uses of personal data is particularly problematic in the social sciences research context where there is a dearth of legal guidance or critical interpretation of the legality requirement, outwith

---

[31] Judith Strobl, Emma Cave and Tom Walley, 'Data Protection Legislation: Interpretation and Barriers to Research' (2000) 321 BMJ 890; Tom Walley, 'Using Personal Health Information in Medical Research' (2006) 332 BMJ 130; Graeme Laurie and Nayha Sethi, 'Information Governance Of Use Of Health-Related Data In Medical Research In Scotland: Current Practices And Future Scenarios' (The University of Edinburgh 2011) Working Paper No. 1 <http://www.scot-ship.ac.uk/sites/default/files/Reports/Working_Paper_1.pdf>; David Erdos, 'Systematically Handicapped? Social Research in the Data Protection Framework' (2011) 20 Information and Communications Technology Law 83; David Erdos, 'Stuck in the Thicket? Social Research under the First Data Protection Principle' (2011) 19 International Journal of Law and Information Technology 133; David Erdos, 'Constructing the Labyrinth: The Impact of Data Protection on the Development of "Ethical" Regulation in Social Science' (2012) 15 Information Communication and Society 104.

[32] Notwithstanding the following contributions which have influenced my thinking in this area: Robert Dingwall, 'The Ethical Case against Ethical Regulation in Humanities and Social Science Research' (2008) 3 21st Century Society: Journal of the Academy of Social Sciences 1; Erdos, 'Systematically Handicapped? Social Research in the Data Protection Framework' (n 31); Erdos, 'Stuck in the Thicket? Social Research under the First Data Protection Principle' (n 31); Erdos, 'Constructing the Labyrinth: The Impact of Data Protection on the Development of "Ethical" Regulation in Social Science' (n 31); Andrew Charlesworth, 'Data Protection, Freedom of Information and Ethical Review Committees' (2012) 15 Information, Communication & Society 85.

[33] Although in the UK, the DPPSPD 2000 para 9 provides a legal ground for processing *sensitive* personal data for research if it is in the substantial public interest and meets other safeguarding conditions. There is no equivalent condition to processing *ordinary* personal data for research purposes.

[34] Although the DPD and DPA 1998 provide exemptions for research from compliance with certain provisions, including subject access and data minimisation. Art 13(2), DPD; s 33, DPA 1998.

[35] The second data protection principle, underlying both the DPD and DPA, is that of purpose specification and limitation. This principle requires that personal data are only 'collected for specified, explicit and legitimate purposes [purpose specification] and not further processed in a way incompatible with those purposes [purpose limitation]' (emphasis added). The reuse of personal data for research purposes is given an exemption from the purpose limitation requirement in the DPD, Art 6 6(1)(b) and the DPA s 33(2). I analyse the impact of purpose limitation on reuses of personal data for research in Chapter 2.

recommendations[36] to rely upon individual consent or anonymisation.[37] Even if many social sciences research projects are funded and carried out based on the promise of societal benefit and impact, the public interest conditions are disfavoured due to legal uncertainty regarding the scope and practical application of the public interest concept. The (legally and ethically) acceptable boundaries for applying the public interest conditions to research remain unknown. There is no legal precedent 'testing' the legality requirement in this context. How do data controllers prove the 'public interest' in their processing, if it has not happened yet? And what 'proof' will be sufficient?

This uncertainty has fuelled a 'culture of caution', manifested in overly restrictive interpretations of the DPA 1998.[38] A key example of this is the focus in research governance on obtaining informed consent, whereby the only alternative is considered to be the anonymisation of data – known familiarly as the consent-or-anonymise paradigm.[39] It is important to recognise this as the legal fallacy it is, given that the neither the DPD nor the DPA 1998 creates an explicit or implicit preference for consent – it is merely *one* of several avenues to legality. On the other hand, any

---

[36] Consent is treated as a 'standard' requirement for undertaking ethical social sciences research by leading stakeholders in the UK. JISC, 'Processing Personal Data' (2014) <https://www.jisc.ac.uk/guides/data-protection-and-research-data/processing-personal-data>; 'ESRC Framework for Research Ethics - Updated January 2015' (2015) <http://www.esrc.ac.uk/_images/framework-for-research-ethics_tcm8-33470.pdf>; UK Data Archive, 'Consent' (2016) <http://www.data-archive.ac.uk/create-manage/consent-ethics/consent>.

[37] Additionally, the 'legitimate interests' condition is often recommended as an alternative to consent despite evidence that this condition is not applicable to public authorities, which under the UK includes universities (DPA, Part 1, s 1 and Sch 1, The Freedom of Information Act 2000 or a Scottish public authority as defined in Sch 1, The Freedom of Information (Scotland) Act 2002). EU case law supports this contention by providing that outwith consent, public authorities must rely upon Art 7(c) or (e) in the DPD, the equivalent of either Sch 2, para 3 (a legal obligation) or Sch 2, para 5 (exercise of a discretionary power) under the DPA 1998. Furthermore, under the final text of the GDPR the non-applicability of the legitimate interest provision to processing is confirmed in Art 6(1)(f).

[38] Walley (n 31) 130; Richard Thomas and Mark Walport, 'Data Sharing Review Report' (2008) <http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/links/datasharingreview.pdf> ; The Academy of Medical Sciences, 'A New Pathway for the Regulation and Governance of Health Research' (2011) <http://www.acmedsci.ac.uk/download.php?file=/images/project/130734957423.pdf>; Laurie and Sethi (n 31) 8–9; Graeme Laurie and Leslie Stevens, 'The Administrative Data Research Centre Scotland: A Scoping Report on the Legal & Ethical Issues Arising from Access & Linkage of Administrative Data' [2014] Edinburgh School of Law Research Paper No. 2014/35 12–23.

[39] See Chapter 2 Sections 2-4. Walley (n 31) 130; Sarah Clark and Albert Weale, 'An Analysis of the Social Values Involved in Data Linkage Studies: Information Governance in Health' (Nuffield Trust 2011) 7–9 <http://www.nuffieldtrust.org.uk/sites/files/nuffield/information_governance_in_health_-_research_report-_aug11.pdf>; Graeme Laurie and Emily Postan, 'Rhetoric or Reality: What Is the Legal Status of the Consent Form in Health-Related Research?' [2012] Medical Law Review 386.

perceived requirement that data must otherwise be anonymised (if consent is *not* obtained) entails adherence to a standard which remains subject to widespread confusion across Member States, with inconsistent interpretation[40] as to what is technically and practically required for data to be considered sufficiently 'de-identified'[41] and thus outside the scope of data protection law. In Chapter 2, I will consider the impact of the consent or anonymise paradigm on the undertaking of social sciences and humanities research.

Overall, while a helpful and potentially recognisable example for those of us working within academia, it is important to acknowledge that the practical impact of legal uncertainty in the research context is but *one* example of a widespread and pervasive overreliance on consent and anonymisation as a means to legal legitimacy under data protection law (e.g. it is also prevalent with commercial enterprises[42] and public authorities[43]).

It is also crucial to understand, however, that my critical assessments are *not* undertaken with the view that data protection law is a mere 'barrier' to be overcome by the right legal advice. The legal uncertainty impacting on data controllers equally impacts upon individual data subjects.[44] Individual consent and anonymisation have been treated as

---

[40] Compare: ICO, 'Anonymisation: Managing Data Protection Risk Code of Practice' (2012) 6 <https://ico.org.uk/media/1061/anonymisation-code.pdf>; Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (2014) WP216 5 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>.

[41] 'De-identified' data is a term used throughout the thesis to refer to data which are anonymised on an individual level (rather than creating aggregate/population level data) and where technical security and procedural mechanisms do not allow data to be traced back to an individual. Therefore, de-identified data are no longer directly or indirectly identifiable to the person processing data (such as a researcher), at least in a procedural and functional sense. This type of 'de-identification' is often deployed in academic research settings where public sector data (or 'administrative data') are used for research purposes. For example, 'Getting Data for Research' (*ADRN*, 2016) <https://adrn.ac.uk/getting-data/de-identification/>.

[42] Bart Custers and others, 'Informed Consent in Social Media Use. The Gap between User Expectations and EU Personal Data Protection Law' (2013) 10 SCRIPTed 435; Bart Custers, 'Click Here to Consent Forever: Expiry Dates for Informed Consent' (2016) 3 Big Data & Society.

[43] Thomas and Walport (n 38); The Law Commission, 'Data Sharing Between Public Bodies - A Scoping Report' (2014) <http://lawcommission.justice.gov.uk/docs/lc351_data-sharing.pdf>.

[44] The terminology used in the DPD and DPA 1998 to refer to the individuals to whom personal data relate to. The DPD, Art 2(a) defines 'data subject' within the definition of personal data: '…any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification

panaceas for the protection of individuals' rights and interests in their data. This is despite research demonstrating that even when consent *is* obtained it is seldom informed or indicative of a data controller fully respecting the rights of a data subject.[45] Furthermore, numerous (successful) scientific attempts at the re-identification of data previously considered 'anonymised'[46] demonstrate clear, residual and potential risks, risks exacerbated by the proliferation of publicly available personal data (e.g. from social media) and the rapid enhancement of data linkage technology.[47] As data collection and processing techniques have evolved over time so too have the risks and potential harms posed to individuals.[48] Given the ubiquitous way in which personal data are now collected, it is unrealistic to expect that the obtaining of consent, at any fixed point in time, can accurately communicate to an individual the full spectrum of

---

number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'. Whereas the DPA 1998, s 1(1) defines 'data subject' in a standalone provision: '…means an individual who is the subject of personal data'.

[45] Roger Brownsword, 'The Cult of Consent: Fixation and Fallacy' (2004) 15 Kings College Law Journal; Solon Barocas and Nissenbaum, Helen, 'On Notice: The Trouble with Notice and Consent' (2009) <https://www.nyu.edu/projects/nissenbaum/papers/ED_SII_On_Notice.pdf>; Graeme Laurie and Shawn Harmon, 'Through the Thicket and Across the Divide: Successfully Navigating the Regulatory Landscape in Life Sciences Research' 2013/30 University of Edinburgh, Research Paper Series; Paolo Balboni and others, 'Legitimate Interest of the Data Controller New Data Protection Paradigm: Legitimacy Grounded on Appropriate Protection' (2013) 3 International Data Privacy Law 244; Custers and others (n 42); Solon Barocas and Helen Nissenbaum, 'Big Data's End Run around Anonymity and Consent' in Julia Lane and others (eds), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (Kindle, CUP 2014).

[46] As provided by Khaled El Emam, a leading authority on anonymisation techniques, the term 'de-identification' is used more frequently in North America whereas 'anonymisation' is used more frequently in Europe. In line with El Emam's analysis, I use these terms interchangeably to refer to the *process* of de-identifying data. However, throughout the thesis I refer to my particular definition for 'de-identified data' (note 41 above) when discussing data that results from the application of a specific anonymisation/de-identification process. Khaled El Emam, Sam Rodgers and Bradley Malin, 'Anonymising and Sharing Individual Patient Data' (2015) 350 BMJ : British Medical Journal 1.

[47] Michael Barbaro and Tom Zeller, 'A Face Is Exposed for AOL Searcher No. 4417749 - New York Times' <http://www.nytimes.com/2006/08/09/technology/09aol.html?pagewanted=all&_r=0>; Arvind Narayanan and Vitaly Shmatikov, 'De-Anonymizing Social Networks', *30th IEEE Symposium on Security & Privacy* (2009) <https://www.cs.utexas.edu/~shmat/shmat_oak09.pdf>; Melissa Gymrek and others, 'Identifying Personal Genomes by Surname Inference' (2013) 339 Science 321; Latanya Sweeney and Ji Su Yoo, 'De-Anonymizing South Korean Resident Registration Numbers Shared in Prescription Data' [2015] Technology Science.

[48] Judith Rauhofer, 'Round and Round the Garden? Big Data, Small Government and the Balance of Power in the Information Age' (2014) 2014 University of Edinburgh, School of Law Research Paper Series; Kate Crawford and Jason Schultz, 'Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms' (2014) 55 BCL Rev. 93; Katherine J Strandberg, 'Monitoring, Datafication, and Consent: Legal Approaches to Privacy in the Big Data Context', *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (Kindle Edition, CUP 2014); Graeme Laurie and others, 'A Review of Evidence Relating to Harm Resulting from Uses of Health and Biomedical Data' (Nuffield Council on Bioethics and Wellcome Trust Expert Advisory Group on Data Access 2015) <http://nuffieldbioethics.org/project/biological-health-data/evidence-gathering/>.

these risks and harms, not to mention the remote likelihood that 1) individuals will take the time to read the associated information 2) fully comprehend it or 3) have meaningful alternative options other than the disclosure of their data.

The consent-or-anonymise paradigm unduly inhibits more holistic consideration of the protection of individuals' rights and interests in their data, as data collection, processing and reuse practices continue to evolve over time and consequently present new types of risks and potential harms. However, this paradigm equally hinders fuller consideration of the potential *benefits* and public interests to be reaped by certain uses of personal data. The dual aims of data protection law are inclusive of two broad public interests – the protection of informational privacy *and* in certain uses of personal data. Current approaches which rely on consent or anonymisation to satisfy the requirements of data protection law are arguably misguided and unable to fully attend to these public interests.

4. Scope and Contribution

This thesis offers a new understanding of the public interest concept as applied to the context of data processing, grounded in extensive legal and theoretical analysis. I suggest legislative amendments and new procedures that can be used to deploy this new understanding of the concept in a way that facilitates both the public interests in protecting informational privacy *and* in certain uses of personal data. While any discussion of the public interest as a justification for processing is often focused on the idea of 'proving' the public interest in the proposed data use, I argue that the public interest is not capable of being 'located' or 'proven' in a singular and static way. It is, and always will be, a highly *contested* concept[49] that can only be established through open

[49] The idea of an 'essentially contested concept' was developed by W B Gallie in 1955 and refers to 'concepts the proper use of which inevitably involves endless disputes about their proper uses on the part of their users.' Mansbridge, as do other theorists, use Gallie's concept 'essentially contested' to analyse the public interest. See Chapter 4, Section 2. WB Gallie, 'Essentially Contested Concepts' (1955) 56 Proceedings of the Aristotelian Society 167, 168–169; Jane Mansbridge, 'On the Contested Nature of the Public Good' in Walter W Powell and Elisabeth S Clemens (eds), *Private Action and the Public Good* (YUP 1998); Ian O'Flynn, 'Deliberating About the Public Interest' (2010) 16 Res Publica 299.

dialogue amongst and on behalf of the relevant 'publics'[50] who may be affected by the data processing in question.

> **The original contribution of this thesis is to offer a legally and theoretically sound basis for data controllers to engage in discussions and considerations of the public interest as applied to their processing of personal data, where the public interest may be used to justify processing. I also suggest ways in which the ICO and courts would assess data controllers' initial determination that their processing is justifiable in the public interest.**

While it is not my aim (and arguably not possible) to define the public interest exhaustively, data protection law uses the concept at important legal junctures without providing appropriate mechanisms to deploy it consistently with the aims of the legislation. The public interest is a critical legal concept in data protection that can be used to support and facilitate cooperative behaviour, and thus enable publicly beneficial uses of data, but is justifiable in that role only insofar as informational privacy is also protected and recognised as equally serving a distinct public interest. The approach developed in this thesis is capable of doing just this.

4.1 Audience

This thesis was undertaken with the research context in mind (social sciences research in particular), with a view to improving understandings of data protection law and its requirements in this context and therefore to positively impact the undertaking of research which serves the public interest. Nevertheless, the findings and insights generated have far wider application – to medical research, commercial and third sector research and for any use of personal data which may be justifiable based on the public interest conditions. Indeed, under UK data protection law, neither the concept of the public interest nor research is used solely in regards to the public sector but encompasses the commercial and third sectors as well.[51] Thus, the audience for this

---

[50] The idea of the 'public' or 'publics' in the public interest is understood here to encompass both the ideas of 'a' public as 'a concrete audience, a crowd witnessing itself in visible space, as with a theatrical public' and 'the' public as 'a kind of social totality … thought to include everyone within the field in question.' See Chapter 4 and Chapter 6 Section 3.1. Michael Warner, 'Publics and Counterpublics' (2002) 14 Public Culture 49, 49–50.

[51] Per the DPA 1998 Sch 2 para 5(d), the public interest condition to processing ordinary personal data may be satisfied 'by any person'. Under s 33 of the DPA 1998, research is broadly defined as including: 'statistical or historical purposes'. As discussed in Chapter 3, the scope of 'research' processing is

work includes individuals and organisations engaged in research (regardless of sector) but also data protection practitioners, data protection supervisory authorities and the courts.

4.2 Geography

The geographical context of my thesis is UK-centric but draws upon European primary and secondary resources given the connection between Member State data protection law as the required legislative implementation of the DPD. This connection with the EU is also relevant given the forthcoming GDPR, which despite the UK's 2016 European Referendum result, will come into force for a period in 2018 until the completion of UK exit negotiations from the EU.[52] The thesis is therefore written per the *current* state of the law under the UK's DPA 1998. However, where relevant, references will be made to provisions of the GDPR and how it may impact the status quo.

4.3 Research methods

This thesis is founded upon desk-based research from UK and EU sources within the fields of data protection and human rights law, information and research governance and political and legal theory on the public interest. Although there are clear legal cases of overlap between data protection law and 'privacy' as a human right under the ECHR, my focus is on the public interest conditions within UK and European data protection law. When relevant, I draw upon literature from other jurisdictions, most notably the US, a country with a rich history of debate and discourse surrounding the public interest concept. To inform my legislative and procedural suggestions made in Chapter

---

inclusive of a wide array of purposes, including social sciences research per the discussions in the DPD's *travaux préparatoires*.

[52] The UK Government confirmed this in October 2016: 'We will be members of the EU in 2018 and therefore it would be expected and quite normal for us to opt into the GDPR and then look later at how best we might be able to help British business with data protection while maintaining high levels of protection for members of the public.' 'Oral Evidence - Responsibilities of the Secretary of State for Culture, Media and Sport' (24 October 2016) <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/culture-media-and-sport-committee/responsibilities-of-the-secretary-of-state-for-culture-media-and-sport/oral/42119.html>.

6, I draw upon the Australian experience in authorising public interest uses of personal data.

I have undertaken extensive work to examine the legislative history of the DPD and DPA 1998 to analyse underexplored interpretations of the public interest concept in data protection law and the relationship of the public interest provisions to processing personal data for research. The conceptual gaps on the public interest that I have identified in the law have been 'filled' through significant research into public interest 'theory' spanning both historical (e.g. Plato, Hobbes[53], Hume[54] and Bentham[55]) and more contemporary accounts of the concept (e.g. Sorauf[56], Barry[57], Held[58] and Bozeman[59]). This combination of research into the legislative history on the public interest conditions and theoretical work on the concept is a novel undertaking in data protection, and in its application to the social sciences research context. The legal analysis of common and distinguishing features of the public interest as deployed in analogous areas of law, namely copyright, whistleblowing and freedom of information, is also an original undertaking when contrasted with data protection.

Furthermore, a significant amount of supplementary evidence has been provided through my ongoing work with researchers, public authorities and regulators as a Research Fellow for the UK's ESRC-funded Administrative Data Research Centre Scotland ('ADRC-S').[60] This work and my involvement in consultancy projects for organisations such as NHS Education for Scotland, the Nuffield Council on Bioethics and Wellcome Trust's Expert Advisory Group on Data Access, has contributed to my

---

[53] Thomas Hobbes, *Leviathan* (iTunes edition, Public Domain 1679).
[54] David Hume, *An Enquiry Concerning the Principles of Morals* (Eighteenth Century Collections Online, Gale 2004).
[55] Jeremy Bentham, *An Introduction to the Principles of Morals and Legislation* (Dover edition, Dove Publications, Inc 2007).
[56] Frank Sorauf, 'The Public Interest Reconsidered' (1957) 19 Journal of Politics 616.
[57] Brian Barry, *Political Argument* (Routledge & Kegan Paul 1965).
[58] Virginia Held, *The Public Interest and Individual Interests* (Basic Books 1970); Virginia Held, 'Justification: Legal and Political' (1975) 86 Ethics 1; Virginia Held, *Rights and Goods: Justifying Social Action* (2nd edn, University of Chicago Press 1989).
[59] Barry Bozeman, *Public Values and Public Interest: Counterbalancing Economic Individualism* (iTunes Edition, Georgetown University Press 2007).
[60] 'Administrative Data Research Centre Scotland' <http://adrn.ac.uk/centres/scotland>.

knowledge and experience in applying data protection law to both the social sciences and biomedical research context.

Below I provide a brief outline of the remaining chapters of this thesis.

4.4 Thesis outline

Chapter 2: The Need to Develop the Public Interest Conditions for Processing: The Downside of Current Paradigms of Compliance

In Chapter 2 I examine the reasons behind the predominance of the consent-or-anonymise paradigm and its negative impact on the protection of informational privacy and on the undertaking of social sciences and humanities research.

Chapter 3: Tracing the History and Application of the Public Interest in Data Protection Law – a UK and European Perspective

In Chapter 3 I provide a deep analysis of the legislative history to the DPD and DPA 1998 to examine the purpose and scope of the public interest conditions.

Chapter 4: Reviving the Public Interest Concept in Data Protection Law

In Chapter 4 I expand my legal and theoretical analysis beyond data protection law to address the gaps in understanding the meaning of the public interest concept.

Chapter 5: Apples and Oranges? (In)consistencies of the Public Interest Concept in Freedom of Information, Copyright and Whistleblowing Law

In Chapter 5 I consider the use of the public interest in analogous areas of law to further develop a conceptual and practical understanding of what is required to successfully deploy the public interest in legal settings.

Chapter 6: Key Components and a New Approach to Making Public Interest Determinations in Data Protection Law

Based on the legal and theoretical analysis undertaken, I set forth key components to understanding the public interest in data protection and propose legislative amendments and procedures for deploying this new understanding.

Chapter 7: The Meaning, Value and Utility of the Public Interest Concept for Data Protection Law

I conclude the thesis by summarising how the new understanding and approach to the public interest concept developed can improve data protection law and practice in relation to research uses of data.

Chapter 2 The Need to Develop the Public Interest Conditions for Processing: The Downside of Current Paradigms of Compliance

1. Introduction

This thesis offers a novel analysis of the public interest concept in data protection. The approach I will develop for analysing the public interest will shed light on currently unresolved questions regarding the resolution of tensions between protecting informational privacy and using personal data. The uncertainty which surrounds the public interest concept in data protection impacts negatively upon data subjects and data controllers. Under what conditions *can* a public, private or third-sector entity process personal data because it is deemed to be 'in the public interest'? And by *whom*, and *how*, should this be decided? These are the questions I am most concerned with in this thesis and which are the focus of my contribution: to enhance the understanding of the public interest concept in data protection.

Although the public interest is often invoked rhetorically to support various data initiatives,[61] the actual legal provisions (in the DPA 1998) permitting the processing of

[61] For example, new research initiatives which require access to personal (or de-identified) data often describe the intended use of data in terms of the public interests served: 'Benefits of Administrative Data' (*Administrative Data Research Network*, 2016) <https://adrn.ac.uk/admin-data/benefits/>; 'What Happens to Your Health Data?' (*The Farr Institute of Health Informatics Research*) <http://www.farrinstitute.org/public-engagement-involvement/what-happens-to-your-health-data>. As a further example, the public interest in national security is often invoked in the context of justifying surveillance and the bulk collection of data, such as with the controversial Investigatory Powers Bill: 'Investigatory Powers Bill' (*GOV.UK*, 7 June 2016) <https://www.gov.uk/government/collections/investigatory-powers-bill>; 'Investigatory Powers Bill: May Defends Surveillance Powers' (*BBC News*, 15 March 2016) <http://www.bbc.co.uk/news/uk-politics-35810628>; '"Leaked Report" Reveals Mass Data Fears' (*BBC News*, 7 June 2016) <http://www.bbc.co.uk/news/technology-36469351>; 'Majority of UK MPs Back Investigatory Powers Bill in Vote' (*Out-law.com: legal news and guidance from Pinsent Masons*, 8 June 2016) <http://www.out-law.com/en/articles/2016/june/majority-of-uk-mps-back-investigatory-powers-bill-in-vote/>.

personal data on the basis of the public interest are rarely used in favour of the perceived 'safe' approach to data protection compliance, namely by obtaining individual consent or anonymising data prior to use.[62] Indeed, since the enactment of the DPA 1998, interpretation of the law has been plagued by a 'culture of caution'[63] – risk averse interpretations and cautious data practices (although such 'caution' seemingly has had no impact on the prevalence of data security breaches, particularly by UK public authorities[64]). When data controllers consider their legal basis for using and sharing data for new purposes, the legal provisions requiring an exercise of discretion are often avoided for what are perceived as more straightforward means of compliance: seeking consent or anonymising data. Having data subjects tick-a-box to consent or anonymising data is perceived as simpler and safer (from a liability perspective) than engaging in uncertain balancing exercises weighing the rights and public interests in a given data processing context.

This consent-or-anonymise paradigm of data protection has been criticised[65] as being incapable of comprehensively addressing the rights and interests at stake; both in terms of individuals' rights and interests in their data, and the public interests in 1) safeguarding privacy and 2) in processing data. Informational privacy is often treated as *oppositional* to the public interest in a use of data. Moreover, the 'fetishisation of

---

[62] See Section 4 below.

[63] See Section 2 below. House of Lords, Science and Technology Committee, '2nd Report of Session 2008-09, Genomic Medicine' (2009) para 6.15 <http://www.publications.parliament.uk/pa/ld200809/ldselect/ldsctech/107/107i.pdf>; Nayha Sethi and Graeme T Laurie, 'Delivering Proportionate Governance in the Era of eHealth: Making Linkage and Privacy Work Together' (2013) 13 Medical Law International 168, 172–173; Graeme Laurie and Leslie Stevens, 'Developing a Public Interest Mandate for the Governance and Use of Administrative Data in the United Kingdom' (2016) 43 Journal of Law and Society 360, 362–365.

[64] For example, the UK's health sector (including NHS trusts) continues to account for the most data breach incidents reported to the ICO. 'Data Security Incident Trends' (*ICO*, 2 December 2016) <https://ico.org.uk/action-weve-taken/data-security-incident-trends/>; Leslie Stevens and others, 'Dangers from Within? Looking Inwards at the Role of Maladministration as the Leading Cause of Health Data Breaches in the UK', *Data Protection and Privacy: (In)visibilities and Infrastructures* (Springer 2017).

[65] Criticised in context of genetic, biomedical and social sciences research: Laurie (n 28) 279–296; Elizabeth Murphy and Robert Dingwall, 'Informed Consent, Anticipatory Regulation and Ethnographic Practice' (2007) 65 Informed Consent in a Changing Environment 2223; Dingwall (n 32); Lee A Bygrave and Dag Wiese Schartum, 'Consent, Proportionality and Collective Power' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer 2009); Mark Taylor, 'Health Research, Data Protection, and the Public Interest in Notification' (2011) 19 Medical Law Review 267; Heather Widdows, 'The Individualist Assumptions of Ethical Frameworks', *The Connected Self: The Ethics and Governance of the Genetic Individual* (CUP 2013); Barocas and Nissenbaum (n 45).

consent',[66] for example, can wrongly characterise a perfectly lawful, ethical (and publicly beneficial) form of data processing as 'unlawful' or 'unethical' (or both) if consent is not obtained, even though consent is neither legally necessary under the DPA 1998 nor ethically sufficient to provide robust data protection to individuals. Nevertheless, the consent-or-anonymise paradigm reflects the dominant means of compliance with data protection law and this impacts upon stakeholders' understanding of 1) what the relevant interests are and 2) how to best resolve the tensions between protecting and using personal data.

Section 2 begins by considering why the consent-or-anonymise paradigm has dominated compliance efforts in the UK, reflecting upon the culture of caution and its role in influencing data protection practices. Section 3 unpacks the paradigm further to demonstrate why this approach to data protection is detrimental to the protection of individuals' informational privacy. Section 4 continues by considering the impact upon public interest uses of data from the context of research. In examining the consent-or-anonymise paradigm, and the lack of meaningful engagement with the public interest route to processing, it becomes clear that the public interest conditions are an underexplored area of data protection.

2. The Culture of Caution and the Dominance of the Consent-or-Anonymise Paradigm

Navigating the UK's DPA 1998 has been likened to weaving one's way through a thicket[67] and described as '… a cumbersome and inelegant piece of legislation.'[68] It is not insignificant that these statements were made by judges (in this case Mr Justice Morland and Lord Phillips). If the DPA 1998 is cumbersome for the legal experts of the UK, what of the countless data controllers *without* expert legal advice, who must take decisions based on this legislation on a frequent, if not daily basis? What impact

[66] A phrase coined by Brownsword. Brownsword (n 45); Laurie and Postan (n 39).
[67] *Naomi Campbell v Mirror Group Newspapers* [2002] EWHC 499 (QB), [72] (Morland J).
[68] *Naomi Campbell v Mirror Group Newspapers* [2002] EWCA Civ No: 1373, [72] (Phillips LJ).

does this have on the protection of individuals' informational privacy and on the undertaking of publicly beneficial forms of data processing, such as research?

2.1 Unpacking the culture of caution

Since the enactment of the DPA 1998, the UK Government has commissioned various evidence reviews to assess the efficacy and impact of data protection law on particular sectors of activity. Of relevance to this thesis is Thomas and Walport's 2008 'Data Sharing Review Report', and the more recent 2014 England and Wales' Law Commission report 'Data Sharing Between Public Bodies - A Scoping Report'.[69] The topic of 'data sharing' is of significance given that increasingly, researchers rely upon data which have been originally collected for other purposes and thus require data controllers to share data with them. Both reports contain evidence from consultation responses and in-person meetings with data controllers and other stakeholders across the UK.[70] Overwhelmingly, the evidence revealed a culture of caution surrounding decisions to share or reuse data, within the UK's public sector in particular.

The term a 'culture of caution' was coined by Scotland's current Chief Science Officer Professor Andrew Morris, when he gave evidence to the House of Lords Science and Technology Committee for their 2008-09 Session.[71] Regarding the regulation of the Generation Scotland Project, which provides 'a bioresource of human biological samples available for medical research' from 30,000 individuals across Scotland,[72] Professor Morris commented:

> The Department of Health guidance suggests that this domain is affected by 43 relevant pieces of legislation. There were 12 sets of relevant standards and

[69]Thomas and Walport (n 38); The Law Commission (n 43).

[70] Thomas and Walport's review covered all sectors (public, private and voluntary) and the entirety of the UK, whereas the Law Commission focused solely on data sharing between public authorities in England and Wales. Both report views from data controllers, data protection professionals (such as data protection officers and legal counsel) and other stakeholders including researchers, academics with interest and expertise in data protection, healthcare providers and so forth. Thomas and Walport (n 38) 11–12; The Law Commission (n 43) 3–5.

[71] The report summarises the evidence received and an analysis of the legal, ethical and social (among other) issues surrounding genomic medicine and the undertaking of associated research. 'Oral Evidence' (*UK House of Lords, Science and Technology Committee, 2nd Report of Session 2008-09*, 2009) 58 <www.publications.parliament.uk/pa/ld200809/ldselect/ldsctech/107/107i.pdf>.

[72] The University of Edinburgh, 'Generation Scotland - General Information' (2016) <http://www.ed.ac.uk/generation-scotland/about/general-information>.

> eight professional codes of conduct. *What this has bred is a culture of caution, confusion, uncertainty and inconsistency ... so for us to interpret it and to have consistent interpretation from legal bodies who have data protection responsibilities is absolutely key.* Currently this is the major issue in terms of the ability to safely link data in a way which is in the public good with appropriate security.[73]

Although Professor Morris' comment was made in specific reference to the overlapping regulatory regimes applicable to biomedical research, the culture of caution resulting (at least in part[74]) from legal complexity and ambiguity is also apparent in data practices far beyond this particular context. Thomas and Walport, whose review focused on uncovering barriers to data sharing between and across sectors, found that data controllers were operating within a fog of confusion surrounding the legal framework for data sharing resulting in a culture that is risk averse.[75] Decisions to share data were eventually made but not without agonising delays which Thomas and Walport cited as 'unacceptable' given that they found few examples where the barriers (legal, resource, cultural or otherwise) to data sharing were insurmountable.[76] Although often cited as the critical barrier to data sharing, they '… found that in the vast majority of cases, the law itself does not provide a barrier to the sharing of personal data.'[77] To overcome barriers to data sharing, Thomas and Walport suggest an approach to decision-making based on the principle of proportionality, defined as:

> … the application of objective judgement as to whether the benefits outweigh the risks, using what some might call the test of reasonableness or common sense. Proportionality involves making a considered and high-quality decision based on the circumstances of the case, including the consequence of not sharing. Decisions must flow especially from the principles of relevance and necessity and *the need to avoid an excessive approach.*[78]

---

[73] 'Oral Evidence' (n 71) 58 (emphasis added).
[74] In research conducted for the ADRC-S, my colleague Professor Graeme Laurie and I have identified other key factors contributing to the culture of caution. For example, resource constraints, shortage of relevant technical and legal expertise, concerns with liability and reputational damage, are all factors, which in addition to legal complexity and uncertainty, contribute to cultures of caution surrounding the use and sharing of data. Graeme Laurie and Leslie Stevens, 'Developing a Public Interest Mandate for the Governance and Use of Administrative Data in the United Kingdom' (2016) 43 Journal of Law and Society 360, 383; Graeme Laurie and others, 'From a Culture of Caution to a Culture of Confidence: Lessons Learned from Implementing the Public Records (Scotland) Act 2011 - Workshop Report' (2016) <http://www.nrscotland.gov.uk/files//record-keeping/public-records-act/prsa-adrc-report.pdf>.
[75] Thomas and Walport (n 38) 35–39; 54.
[76] ibid 54.
[77] ibid i.
[78] ibid 14 (emphasis added).

If Thomas and Walport's extensive evidence gathering and engagement did not reveal insurmountable barriers to data sharing, the 'agonising' delays cited by consultees suggests that decision-making processes were *not* proportionate to the risks and benefits of the data sharing in question. In Section 4 below I consider the impact of the consent-or-anonymise paradigm – a manifestation of the culture of caution – on the undertaking of research.

Like Professor Morris, Thomas and Walport cited the complex and overlapping legal regimes as a key contributing factor to the difficulties faced in taking decisions on data sharing, specifically referencing the ambiguity surrounding practical interpretation of the DPA 1998.[79] Similar views were echoed six years later in the evidence gathered by England and Wales' Law Commission; several public sector consultees did not find the DPA 1998 readily understandable[80] citing various parts of the legislation which were particularly confusing to implement. This included references to difficulties faced by data controllers in interpreting the meaning of 'necessary' as it applied to various conditions for processing in Schedules 2 and 3; questions over when it was appropriate

[79] Barriers to data sharing stemming from inconsistent interpretation of data protection laws and legal 'grey areas' are problematic in jurisdictions far beyond the UK including in Australia, New Zealand and the US. J Ramon Gil-Garcia, InduShobha Chengalur-Smith and Peter Duchessi, 'Collaborative E-Government: Impediments and Benefits of Information-Sharing Projects in the Public Sector' (2007) 16 European Journal of Information Systems 121; Thomas and Walport (n 38) 22, 35–36; Christine M O'Keefe and Chris J Connolly, 'Privacy and the Use of Health Data for Research' (2010) 193 The Medical Journal of Australia 537; Jane Fedorowicz, Janis L Gogan and Mary J Culnan, 'Barriers to Interorganizational Information Sharing in E-Government: A Stakeholder Analysis' (2010) 26 The Information Society 315; AMB Lips, RR O'Neill and EA Eppel, 'Cross-Agency Collaboration in New Zealand: An Empirical Study of Information Sharing Practices, Enablers and Barriers in Managing for Shared Social Outcomes' (2011) 34 Int J Public Adm; Jussi Sane and Michael Edelstein, 'Overcoming Barriers to Data Sharing in Public Health: A Global Perspective' (Chatham House: The Royal Institute of International Affairs 2015) <https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20150417OvercomingBarriersDataSharingPublicHealthSaneEdelstein.pdf>; Elizabeth Green and others, 'Enabling Data Linkage to Maximise the Value of Public Health Research Data' (Wellcome Trust 2015) <https://wellcome.ac.uk/sites/default/files/enabling-data-linkage-to-maximise-value-of-public-health-research-data-phrdf-mar15.pdf>.

[80] The Law Commission (n 43) 53.

to apply the section 33 research exemption;[81] and how to determine whether data have been sufficiently anonymised to be taken outside the scope of data protection law.[82]

2.2 Legal ambiguity

The evidence gathered in both reports indicates widespread difficulties for data controllers in interpreting provisions of the DPA 1998, specifically where bright line rules do not apply (or are not provided) and an exercise of discretion is needed. For example, uncertainty arises when determining whether it is 'necessary' to share data, and if so, under what authority and what conditions sharing should occur. As provided by Thomas and Walport, the data protection principles in Schedule 1 of the DPA 1998 are: 'sound, balancing individual protection against the wider need to process and share information. They provide a sensible approach to handling and processing data, *neither inhibiting nor promoting data sharing*.'[83] The problem lies in *applying* the principles in practice: '… the Data Protection Act does not, and maybe by itself cannot, provide a sufficiently practical framework for making decisions about whether and how to share personal data.'[84]

The applicability of key provisions, notably the conditions for processing, rest upon the interpretation of concepts such as 'necessary' and the 'public interest' that are not defined in the DPA 1998. It is also unclear how other principles should apply to such determinations, notably the European jurisprudential principle of 'proportionality' that is referenced in UK cases where the 'necessity' of processing is considered. [85]

---

[81] Which exempts the processing of ordinary personal data from complying with the second and fifth data protection principles and from subject access requests, so long as 1) the processing is not used to take decisions on individuals and 2) is unlikely to cause substantial damage and distress to the data subjects or any other person. Although not an exemption, the DPPSPD 2000 provides a legal basis for processing sensitive personal data for research purposes so long as it is 1) in the substantial public interest; 2) is 'necessary' for research purposes; 3) is not used to take decisions on individuals and 4) does not cause or is not likely to cause substantial damage or distress to the data subject or any other person. The DPPSPD 2000 was enacted by the UK per the derogations allowed by Article 8(4) of the DPD.

[82] The Law Commission (n 43) 53–54.

[83] Thomas and Walport (n 38) 36 (emphasis added).

[84] ibid.

[85] For example: *R v Secretary of State for the Home Department (ex parte Daly)* [2001] UKHL 26 [26]-[27] (Steyn LJ); *R (Ellis) v Chief Constable of Essex Police* [2003] EWHC 1321 (Admin) [1], [27]-[29] (Goldring J); *Stone v South East Coast Strategic Health Authority* [2006] EWHC 1668 (Admin)[60] (Davis J); *Corporate Officer of the House of Commons v The Information Commissioner and Others* [2009] 3 All ER 403 [59]; *R (on the*

Proportionality is neither specifically referenced in the DPA 1998 nor uniformly interpreted by UK Courts. In such circumstances, authoritative guidance could enhance data controllers' confidence when taking decisions regarding data sharing which can help facilitate the use and sharing of data when it is in the public interest to do so. However, in the specific context of the use and sharing of data for *research*, that is the focus of this thesis, the legislation has *not* been tested and a myriad of sometimes conflicting professional, governmental and academic guidance proliferate.[86]

Undoubtedly it is because the DPA 1998 applies to *all* processing of personal data within the UK, regardless of purpose or the sector of activity, that its provisions must be broadly formulated and applicable to the widest range of contexts. While it is outside the scope of this thesis to consider the merits of comprehensive data protection legislation versus a sectoral approach to regulation (as applied in the United States)[87], the all-encompassing nature of the DPA 1998 inevitably leaves the legislation open to misinterpretation. I am arguing that the legal ambiguity surrounding key provisions of the legislation, which has gone unresolved for nearly two decades, puts at risk both

---

application of Catt) (AP) (Respondent) v Commissioner of Police of the Metropolis and another (Appellants) [2015] UKSC 9 [6]; *R (AB) v Chief Constable of Hampshire Constabulary* [2015] EWHC 1238 (Admin).

[86] For example, each UK university will have its own data protection guidance for researchers that may differ from the guidance provided by a specific department or school within that university; this guidance might further differ from the guidance provided by a research funder or research centre. Consider the various data protection guidance documents from the University of Edinburgh applicable to researchers, compared to that of the funder for my research fellowship (the ESRC) and provided by my research centre the Administrative Data Research Centre Scotland. The University of Edinburgh, 'Research and the Data Protection Act' (2008) <http://www.ed.ac.uk/records-management/data-protection/guidance-policies/research/act>; The University of Edinburgh, 'Data Protection for Students' (2014) <http://www.ed.ac.uk/records-management/data-protection/guidance-policies/dpforstudents>; The University of Edinburgh, 'University of Edinburgh Data Protection Policy' (2015) <http://www.ed.ac.uk/records-management/data-protection/data-protection-policy>; The University of Edinburgh, 'Research Ethics and Data Protection' (2016) <http://www.ed.ac.uk/records-management/data-protection/guidance-policies/research/ethics>; ESRC, 'Data Protection' <http://www.esrc.ac.uk/funding/guidance-for-applicants/research-ethics/frequently-raised-topics/data-requirements/data-protection/>; ADRN, 'Data Protection Act' <https://adrn.ac.uk/protecting-privacy/legal/dpa/>.

[87] Considered by: Patricia L Bellia, 'Federalization in Information Privacy Law' (2009) 118 Yale Law Journal 868; Paul M Schwartz, 'Preemption and Privacy' (2009) 118 Yale Law Journal; Kenneth A Bamberger and Deirdre K Mulligan, 'Privacy on the Books and on the Ground' (2010) 63 Stanford Law Review 247. See report commissioned by the European Parliament comparing the standard of data protection in EU versus the US in the law enforcement context which provides comprehensive comparisons: European Parliament, 'A Comparison between US and EU Data Protection Legislation for Law Enforcement' (2015) <http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU%282015%29536459_EN.pdf>.

aims of the DPA 1998 – to protect informational privacy *and* facilitate the use of personal data.

In other work, myself and a colleague have argued that the law in itself is not the greatest barrier to data sharing within the UK's public sector; rather, organisational cultural and sector-specific practices surrounding data are far more a hindrance to the use and sharing of data for research purposes.[88] Organisational cultures do fundamentally influence how data are viewed and handled.[89] When cultures of *caution* predominate, decisions are taken from a risk averse position, prioritising the interests and risks perceived as important by a particular data controller organisation, in potential neglect of the wider public (and private) interests at stake. The ambiguity surrounding key provisions of data protection law in the UK contributes to this culture of caution and it is this legal deficiency which I am chiefly concerned with, as it is one which is resolvable through legislative change as opposed to reliance on divergent interpretations or ad hoc judicial decisions. The potential 'success' of legislative changes in this area of data protection law is evidenced by the successful deployment of the public interest concept in analogous areas of UK law and the legislative solutions employed in other common law jurisdictions.[90]

Here, I am directly criticising the law and highlighting what is most problematic for those charged with interpreting and implementing the DPA 1998 on a regular basis. Initially, data controllers are required to determine their legal basis for processing personal data, often without the assistance of legal experts; yet, neither the law nor subsequent guidance has provided them with the interpretative tools to do this. My critique of the law is first based on the unresolved vagueness of terms in key provisions of the DPA 1998, notably those within the Schedules 2 and 3 conditions. These comprise critical provisions that data controllers must demonstrate compliance with if their processing is to be considered lawful. For the purposes of this thesis, there are at

---

[88] Laurie and Stevens, 'Developing a Public Interest Mandate for the Governance and Use of Administrative Data in the United Kingdom' (n 74).
[89] Thomas and Walport (n 38) 2.
[90] See discussion of the deployment of the public interest in analogous contexts in Chapter 5, and discussion of the Australian public interest determination procedure in Chapter 6.

least three research processing scenarios where the data controller must determine on their own, the appropriate legal basis for processing and which the arguments made within this thesis are directed at:

1. Where a data controller collects data themselves for research;
2. Where a data controller seeks to reuse data for research that they *previously collected* for different purposes; and
3. Where a data controller seeks to share data with third parties that will reuse data for research, whereby both the original data controller and third party[91] must have their own separate legal basis (the original data controller must have a legal basis for sharing data, whereas the third party must have a legal basis for processing data for research).

In each of these cases, and indeed any other data use situation, the data controller must determine their legal basis for processing,[92] and the vagueness of the Schedule 2 and 3 conditions to processing make it unclear whether data controllers can rely on anything other than consent when sharing or using data for research purposes.

In reference to *case three* above, where a data controller *shares* their previously collected data for research, the data controller must find an appropriate legal basis for sharing (under Schedule 2 and Schedule 3 if sharing sensitive personal data) **and** ensure that the sharing of data further complies with the other data protection principles in Schedule 1 of the DPA 1998.[93] Importantly, the sharing of data for research, which were originally collected for other purposes, must be not be *incompatible* with the original reasons for collection.[94] (Note that this analysis would also apply to *case two* above, given that a data controller's *own reuse* of data for research would 1) need an

---

[91] Within the research context the receiving data controller (who is in receipt of the previously collected dataset) will often be a University and/or Principal Investigator of a funded research project.

[92] Under the first data protection principle, all processing of personal data must be fair and lawful; this requires satisfying one of the conditions under Schedule 2, if ordinary personal data, or of both Schedules 2 and 3 if sensitive personal data. Therefore, the conditions in Schedules 2 and 3 are fundamental to data controllers satisfying their obligation of lawfulness under the Act. DPA 1998, Sch 1, para 1(a)-(b).

[93] DPA 1998, Sch 1, paras 1-8.

[94] The second data protection principle requires 1) that when personal data are collected, that the purposes for collection be explicitly identified and legitimate (purpose specification) and that 2) any further use of personal data not be incompatible with the purposes for which data were originally collected (purpose limitation). When sharing data with a third party, such as a researcher, that sharing of data must not be incompatible with the reasons why the original data controller collected those data. DPA 1998, Sch 1, para 2.

appropriate legal basis and 2) not be incompatible with their original reasons for collection.)

Focussing on the issue of incompatibility of reuses of data, critically, under both the DPA 1998 and DPD, processing for research is given an exemption from the purpose limitation principle,[95] but importantly, *only if* 1) data are further processed for *only* research purposes **and** 2) the data controller provides the requisite safeguards to data subjects (i.e. data will not be used to take decisions on specific individuals nor will data be used in a way that is likely to cause substantial damage or distress to any data subject).[96] Note, that further uses of data for research are *not* exempt from complying with the *purpose specification principle* – thus data controllers must be satisfied prior to sharing that the purposes for reuse are appropriately specified e.g. the research project would need to be defined in sufficient detail.[97]

The breadth of the research exemption from purpose limitation is called into question by Article 29 Working Party guidance on this issue.[98] For the Working Party, the exemption to purpose limitation for research is *not* absolute and is contingent on the *adequacy* of safeguards provided; the applicability of the exemption is determined from context sensitive analysis in each case, particularly to scrutinise the sufficiency of anonymisation or pseudonymisation techniques deployed so as to minimise any potential impact on specific data subjects.[99] Looking to CJEU case law, there is a lack

---

[95] DPD, Art 6(1)(b); DPA 1998, s 33(2).

[96] DPD, Art 6(1)(b); DPA 1998, s 33(1)-(2), (5). In the UK, these safeguards are called 'the relevant conditions' of Section 33(1). To avail of the research exemptions provided in Section 33, data controllers must comply with these conditions which provide:
(a)that the data are not processed to support measures or decisions with respect to particular individuals, and
(b)that the data are not processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject.

[97] The Article 29 Working Party's guidance on purpose limitation provides that to satisfy the requirement of *purpose specification*, that 'the degree of detail in which a purpose should be specified depends on the particular context in which the data are collected and the personal data involved.' A clear description of the research project, along with information on how data would be processed, by whom and under what conditions, would be required on a practical basis in any event prior to data being shared with a researcher. Article 29 Data Protection Working Party, 'Opinion 03/2013 on Purpose Limitation' (2013) WP203 16 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>.

[98] Article 29 Data Protection Working Party, 'Opinion 03/2013 on Purpose Limitation' (n 97).

[99] ibid 28–32.

of guidance to help assess when safeguards may be considered 'adequate' vis-à-vis reuses of data.

The CJEU has considered this issue tangentially in cases focused on the reuse of data by public authorities (which has some relevance here given the reuse of public sector data for research contemplated throughout this thesis). In *Willems and others*,[100] the Court side-stepped the issue of purpose limitation when it ruled that Council Regulation No 2252/2004/EC (requiring Member States to collect biometric data such as fingerprints to verify the authenticity of travel documents and individual identity) did not oblige Member States to guarantee that such data would not be reused for other purposes.[101] Thus, in *Willems*, the CJEU failed to define what safeguards must be provided to data subjects when national/European law does permit the reuse of personal data for other purposes. In *Bara and others*, the focus was on the right of individuals to information prior to transfers of data between public authorities and *not* on whether the transfer was incompatible under Article 6 of the DPD.[102] While the CJEU provided that such a transfer required a legal basis (under Article 7) and must comply with the principles in Article 6 of the DPD (including purpose limitation), the Court did not ultimately assess the compatibility of the transfer.[103] Thus, the Working Party's Opinion remains the most relevant guidance on the issue for the time being.

From the perspective of the Working Party, it is likely that the *sufficiency* of the 'relevant conditions' or safeguards provided to data subjects in Section 33 of the DPA 1998 would be questioned. Section 33 makes no reference to technical, procedural or organisational safeguards that could be deployed by researchers to minimise any potential impact to specific data subjects.[104] However, it is arguable that these issues are impliedly dealt with and required of a data controller vis-à-vis their compliance with the other data protection principles, notably with the data minimisation principle and technical/organisational security principle.[105]

---

[100] Cases C-446/12 and C-449/12 *Willems and others* [2015], para 48.
[101] ibid paras 47-48.
[102] Case C‑201/14 *Bara and Others* [2015], para 31, 34.
[103] ibid para 30. The transfer of data being between a Romanian tax authority and the national health insurance fund.
[104] Article 29 Data Protection Working Party, 'Opinion 03/2013 on Purpose Limitation' (n 97) 32.
[105] DPA 1998, Sch 1, para 3 and 7. The data minimisation principle comprises the last part of the third data protection principle that 'Personal data shall be adequate, relevant *and not excessive in relation to the*

A further divergence from the UK approach to the research exemption is indicated by the Working Party's view that the further processing of data on health, children, other 'vulnerable' individuals and 'highly sensitive information' should 'in principle' only be reprocessed for research with the *consent* of the data subject.[106] This particular point would be contentious, at least within the UK's research community, given that Section 33 of the DPA 1998 does *not* require different treatment for research processing involving health data, data on children, data on 'vulnerable' individuals or on 'highly sensitive information' (the latter two being undefined terms in either the DPA 1998 or DPD). Moreover, the Working Party qualified their stipulated requirement for consent by stating that 'in principle' research involving such data should not proceed without it. As to the other points made by the Article 29 Working Party, certainly, data controllers must ensure robust safeguards are in place prior to their own reuse of data for research, but particularly so where they share data with third parties for research purposes. Furthermore, the safeguards provided would likely be evaluated (at least outside of the UK) from a broader perspective than whether the relevant conditions of Section 33 of the DPA 1998 were complied with.

Clearly, while there is guidance on these other legal principles that are relevant to the reuse and sharing of data for research, it remains unclear on what legal basis such activity can proceed.[107] The Article 29 Working Party made the important point that

---

purpose or purposes for which they are processed.' The seventh data protection principle on technical and organisational security provides that 'Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.' It could be argued that the type of technical, procedural and organisational safeguards discussed by the Working Party would be deployed in line with a data controller's obligations under these third and seventh principles. Nevertheless, and at least within the UK, a data controller must only satisfy of the relevant conditions stipulated by Section 33(1) of the DPA 1998 to avail of the purpose limitation exemption (even if the adequacy of safeguards is later called into question upon future judicial review of a particular case).

[106] Article 29 Data Protection Working Party, 'Opinion 03/2013 on Purpose Limitation' (n 97) 32.

[107] Outside of reuses of personal data for research, it is far *less* clear whether the sharing and/or reuse of data for purposes other than those for which data were originally collected, would be compliant with the purpose limitation principle. For reuses and sharing of data for secondary purposes *other than research*, a data controller must consider whether that further use of data is incompatible with the reasonable expectations of the data subject in line with the context in which data were originally collected. Again, as to public sector data controllers, they must look at the new purpose for processing and whether it is required by law or otherwise to carry out a task 'in the public interest', which in the latter case the Article 29 Working Party indicate that the public body must undergo this assessment themselves. Article 29 Data Protection Working Party, 'Opinion 7/2003 on the Re-Use of Public Sector Information and the

even if a further use of data for research can satisfy the requirements of purpose limitation, that this further use must still be supported by an appropriate legal basis for processing.[108]

The broad nature and terminology of the DPA 1998, and in particular the wording of Schedules 2 and 3, can:

> …allow too much scope to interpret the Act in different ways, while even the name of the Act gives the misleading impression that organisations should seek to protect information from use by other organisations or for any additional purposes.[109]

Indeed, because of this legal uncertainty, the DPA 1998 is interpreted in a risk averse manner: '…the Act is frequently interpreted too restrictively or over-cautiously due to unfamiliarity, misunderstanding, lack of knowledge or uncertainty about its provisions.'[110] In the context of using, reusing or sharing personal data for research, and specifically in finding the appropriate legal basis to do so under Schedules 2 and 3, this manifests in the predominance of the consent-or-anonymise paradigm as it is perceived as less legally and practically ambiguous. And as discussed above, satisfaction and compliance with the other data protection principles, notably with purpose limitation, is relatively straightforward, considering the research exemptions available in Section 33 of the DPA 1998.[111] Thus, the culture of caution surrounding the use and sharing of data for *research* is likely to lie beyond the interpretation of these other data protection principles, and is at least more likely connected with the ambiguity surrounding the conditions for processing – which again represent the *first* data protection principle – that processing must be lawful. My second basis for critique of the current law, as indicated above, is that such ambiguity is resolvable through legislative amendments, as evidenced from efforts made in other areas of UK law as

---

Protection of Personal Data: Striking the Balance' (n 25) 6–8; Article 29 Data Protection Working Party, 'Opinion 03/2013 on Purpose Limitation' (n 97) 39–40.

[108] Article 29 Data Protection Working Party, 'Opinion 03/2013 on Purpose Limitation' (n 97) 33.

[109] Thomas and Walport (n 38) 36.

[110] ibid.

[111] Section 33 of the DPA 1998 also provides an exemption from the fifth data protection principle (researchers can retain data indefinitely) and from Section 7 which exempts data held solely for research purposes from data subject access requests. DPA 1998, s 33, paras 3-4.

well as in other jurisdictions.[112] Immediately below I consider the detrimental impact of the consent-or-anonymise paradigm on the protection of informational privacy.

3. The Impact of the Consent-or-Anonymise Paradigm on the Protection of Informational Privacy

A key reason why a new approach to data protection compliance is needed is because of the impact of the consent-or-anonymise paradigm on the protection of individuals' informational privacy. This paradigm promotes a brand of data protection, one that equates sufficient protection of informational privacy with the obtaining of consent or the anonymisation of data. On this line of reasoning, individuals' rights and interests in their data are adequately respected if their consent is obtained. Alternatively, if data are anonymised, individuals' rights and interests in their data are no longer engaged. In the analysis below I will demonstrate how neither consent nor anonymisation *on its own* can guarantee that the rights and interests of individuals are adequately protected and thus the inadequacy of current approaches to data protection. I will first consider the fallibility of anonymisation and the extent to which individuals have residual rights and interests in even de-identified data. This discussion is followed by a more extensive analysis of the impact of the fetishisation of consent on protecting individuals' informational privacy and on our understandings of informational privacy as it relates to the public interest.

3.1 Informational privacy beyond identifiability – why anonymisation is not enough

In the data processing context anonymisation can be understood as:

> …ensuring that the probability of assigning a correct identity to a record in a dataset is very small. This probability can be conditional on other factors, such as the skills required and resources available to an adversary seeking to re-identify a record.[113]

---

[112] Discussed in Chapters 5 and 6.
[113] El Emam, Rodgers and Malin (n 46) 1–2; Citing: Khaled El Emam, *Guide to the De-Identification of Personal Health Information* (CRC Press Taylor & Francis Group 2013).

Importantly, El Emam makes clear the technical limits of anonymisation: '[when] data is shared, *it is not possible to ensure that the probability of re-identification is zero*, but it is possible to ensure that the probability is very small.'[114] Thus the reverse of anonymisation is:

> …reidentification or deanonymization. A person, known in the scientific literature as an adversary, reidentifies anonymized data by linking anonymized records to outside information, hoping to discover the true identity of the data subjects.[115]

Under data protection law, if data are considered 'anonymous' they are no longer within the scope of regulation. Anonymisation is not defined in the DPA 1998, but is referred to in Recital 26 of the DPD: 'whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.' This in turn references the concept of *identifiability* which is defined differently in the DPD than under the DPA 1998. The key difference being that the UK has created an 'in the hands of the data controller' concept whereby data subjects are considered identifiable only if identification is possible via data held alone or together with other data *by the data controller* himself.

Under the DPA 1998 data are identifiable to the extent that a living individual 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'.[116] Under the DPD, the data subject is considered identifiable via data held by the data controller if that data is combined with other data held by a third party. This is provided in Recital 26 of the DPD whereby identifiability is defined in terms of '… all the means likely reasonably to be used either by the controller or by any other person to identify the said person.'[117] The consequence of this is that the UK's conception of identifiability could limit the type of data treated as personal data under the DPA 1998 compared to the DPD, a prospect clearly problematic in the age of Big Data and habitual data sharing. To this end, the UK has received criticism since the enactment

---

[114] El Emam, Rodgers and Malin (n 46) 2 (emphasis added).
[115] Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2009) 57 UCLA Law Review 1701, 1707–1708.
[116] DPA 1998, s 1(1).
[117] DPD, Recital 26.

of the DPA 1998 as the legislation has been perceived as a deficient transposition of the Directive, resulting in a lower standard of protection than intended.[118]

Nevertheless, the ICO published its Anonymisation Code of Practice in 2012, which seems to ignore this wording of the DPA 1998 and rejects the 'in the hands of the data controller' concept of identifiability, recognising that the prospect of re-identification must be far broader:

> …"other information" needed to perform re-identification could be information available to certain organisations, to certain members of the public or that is available to everyone because it has been published on the internet, for example.[119]

This interpretation does not hinge on whether data are in the hands of the data controller, but rather the extent to which 'other information' is available to third parties that might identify an individual, aligning itself more closely to the DPD's Recital 26.[120]

Even with this broader understanding of identifiability in mind, the ICO's approach to anonymisation recognises the technical realities of de-identification: '[the] DPA does not require anonymisation to be completely risk free – you must be able to mitigate risk of re-identification until it is remote.'[121] Nevertheless, determining when the risk of re-identification is 'remote' and thus when data are effectively anonymised for the purposes of data protection law remains 'difficult'.[122] The ICO considers this difficulty to revolve around two key issues:

---

[118] Lilian Edwards, 'Taking the "Personal" Out of Personal Data: Durant v FSA and Its Impact on the Legal Regulation of CCTV' (2004) 1 SCRIPTed 341; Chris Pounder, 'Question Answered: "Why Does the European Commission Think the UK's Data Protection Act Is a Deficient Implementation of Directive 95/46/EC?". - Hawktalk' <http://amberhawk.typepad.com/amberhawk/2013/02/question-answered-why-does-the-european-commission-think-the-uks-data-protection-act-is-a-deficient-implementation-of.html>; 'Europe Claims UK Botched One Third of Data Protection Directive' (*Out-law.com: legal news and guidance from Pinsent Masons*) <http://www.out-law.com/page-8472>.

[119] ICO, 'Anonymisation: Managing Data Protection Risk Code of Practice' (n 40) 18.

[120] A point echoed in the ICO's 2012 guidance on determining what is personal data, where they make clear their preference for interpreting personal data in line with the DPD's Recital 26. The ICO, 'Determining What Is Personal Data' (2012) 29 <https://ico.org.uk/media/for-organisations/documents/1554/determining-what-is-personal-data.pdf>.

[121] ICO, 'Anonymisation: Managing Data Protection Risk Code of Practice' (n 40) 16.

[122] ibid.

- the concept of 'identify' – and therefore of 'anonymise' – is not straightforward because individuals can be identified in a number of different ways. This can include direct identification, where someone is explicitly identifiable from a single data source, such as a list including full names, and indirect identification, where two or more data sources need to be combined for identification to take place; and
- you may be satisfied that the data your organisation intends to release does not in itself, identify anyone. However, in some cases you may not know whether other data is available that means that re-identification by a third party is likely to take place.[123]

3.1.1 Regulatory gaps and technology

Not only are the technical boundaries between anonymous versus identifiable data uncertain and difficult to gauge by data controllers, technically speaking, it is becoming far more difficult to ensure re-identification is beyond a remote possibility. This refers to the proliferation of personal and supposedly de-identified data flows, the increasingly sophisticated ways seemingly innocuous data can be combined and 'repackaged' as valuable individual and group profiles for commercial, governmental and more nefarious purposes. Considered in the context of big data, Barocas and Nissenbaum suggest that:

> …even where strong guarantees of anonymity can be achieved, common applications of big data undermine the values that anonymity traditionally had protected. Even when individuals are not 'identifiable', they may still be 'reachable', may still be comprehensibly represented in records that detail their attributes and activities, and may be subject to consequential inferences and predictions taken on that basis.[124]

The law is quickly outpaced in this context. The rapidity with which data processing technology evolves means that any attempt to regulate in this space, based on arbitrary definitions of identifiability, is fruitless. Moreover, it places individuals at risk who will not be able to benefit from the protection of law because their data might be *legally* considered 'anonymised' even if *technically* such data are still re-identifiable. Regulating based on data being identifiable is what Paul Ohm considers to be akin to:

---

[123] ibid. Again this passage from the guidance indicates that the ICO's perspective reflects the DPD's standard of identifiability under Recital 26 and *not* the UK's under the DPA 1998.
[124] Barocas and Nissenbaum (n 45) 45.

> …the carnival whack-a-mole game: As soon as you whack one mole, another will pop right up. No matter how effectively regulators follow the latest reidentification research, folding newly identified data fields into new laws and regulations, researchers will always find more data field types they have not yet covered.[125]

While strides have been made to improve the anonymisation process,[126] any façade of impenetrability has long since been shattered. Ohm's seminal piece on anonymisation describes the nature and gravity of potential harms that can arise from the increasing amount of data available and the technical capabilities to re-identify supposedly anonymous data:

> Almost every person in the developed world can be linked to at least one fact in a computer database that an adversary could use for blackmail, discrimination, harassment, or financial or identity theft. I mean more than mere embarrassment or inconvenience; I mean legally cognizable harm. Perhaps it is a fact about past conduct, health, or family shame. For almost every one of us, then, we can assume a hypothetical database of ruin, the one containing this fact but until now splintered across dozens of databases on computers around the world, and thus disconnected from our identity. Reidentification has formed the database of ruin and given our worst enemies access to it.[127]

To this end, Ohm, Schwartz and Solove advocate for the regulation of personal data that is not hinged upon current understandings of 'identifiability'.[128] As for Ohm, he advocates a risk-based approach to the regulation of data flows, where data are regulated according to the risks of re-identification posed by a particular type of processing.[129] Schwartz and Solove propose a reconceptualisation of identifiability where different levels of regulation attach depending on where data fall on the identifiability spectrum: 1) identified; 2) identifiable; or 3) non-identifiable.[130]

---

[125] Ohm (n 115) 1742.
[126] Notably by: Latanya Sweeney, 'K-Anonymity: A Model for Protecting Privacy' (2002) 10 International Journal on Uncertainty, Fuzziness and Knowledge-based Systems 557; Latanya Sweeney, 'Achieving K-Anonymity Privacy Protection Using Generalization and Suppression' (2002) 10 International Journal on Uncertainty, Fuzziness and Knowledge-based Systems 571.
[127] Ohm (n 115) 1748.
[128] Ohm (n 115); Paul M Schwartz and Daniel J Solove, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information' (2011) 86 New York University Law Review 1814.
[129] Suggesting five factors to assess the risks of re-identification and thus privacy harm: 1) data handling techniques; 2) private versus public release of data; 3) quantity (the size of the database held); 4) motive to re-identify; and 5) trustworthiness of the data custodian. Ohm (n 115) 1764–1768.
[130] Schwartz and Solove (n 128) 1877–1879.

Both approaches attempt to ameliorate the inherent flaws of regulating by hard-and-fast categories of 'personal' versus 'anonymous' data. What is important to recognise for the wider aims of this thesis is that current approaches to data protection, which strongly rely upon anonymisation, are not *on their own* able to offer sufficient guarantees of protection. Because of this uncertainty over what processing is outwith the DPA 1998, data controllers are prodded (at least implicitly, if not at times explicitly) to take the cautious path and obtain individual consent for *all* data processing on the (albeit misconstrued) basis that it might be within the scope of the law.

3.1.2 Interests in data beyond identifiability

To conclude this discussion on anonymisation I want to briefly consider the idea that individuals may have valid, residual rights and interests in data that have been anonymised. If this is so, there are even stronger imperatives to consider and implement wider protections of individuals' data beyond the technical security offered through anonymisation. In the UK, this proposition runs against the current *legal* position. In the English Court of Appeal case, *R v Department of Health, ex parte Source Informatics Ltd.*, the Court held that there could be no breach of confidence if individuals' privacy interests were protected by the anonymisation of their data.[131] On this basis, the Court ruled that individuals did *not* have any legally valid, residual rights and interests in data that have been anonymised. Within the context of genetic research, Laurie convincingly argues *against* this position:

> When anonymisation occurs, the quality of the relationship that an individual has with her sample or her information is reduced, and this permits other interests to weigh more heavily in the balance. *At no point, however, does that relationship cease to exist, for anonymisation is merely a process to ensure security*.[132]

For Laurie, informational privacy is broader than the mere issue of identification. Laurie contends that anonymisation alone 'does not necessarily meet the ethical requirements of respect for individuals' if we consider the *fundamental* interest individuals have with their genetic samples and associated data.[133] What are the nature of these fundamental interests in personal data which go beyond identifiability?

---

[131] [2000] 1 All ER 786 [34]-[35] ('*Source Informatics*').
[132] Laurie (n 28) 294 (emphasis added).
[133] ibid 294–295.

Taylor also explores this question in the context of genetic research, where individuals have demonstrated concerns with the '… (perceived) misuse of the information that genetic research might yield'.[134] When it comes to patient health data, some are considered so 'sensitive' that they should not be reused, such as for research, even if anonymised.[135] In the social sciences context, as to the longitudinal study 'Avon Longitudinal Study of Parents and Children' young people were interviewed about their views on data linkage research; some considered that consent should be required to reuse data for research even if data were anonymised.[136] The interviews revealed issues with trust as interviewees expressed residual concerns about how anonymous data would be handled and the potential for data misuse.[137] For others, anonymisation was not enough to signal respect to research participants, respect that could be engendered through the process of 'being asked':

> Even where this risk could be effectively mitigated through anonymization some individuals still felt it polite that their permission should be sought for secondary use of information they perceived they 'owned'.[138]

Barocas and Nissenbaum focus on the impact that the misuse of supposedly anonymous data can have on individuals:

> In this work, we argued that the value of anonymity inheres not in namelessness, and not even in the extension of the previous value of namelessness to all uniquely identifying information, but instead to something we called 'reachability', *the possibility of knocking on your door, hauling you out of bed, calling your phone number, threatening you with sanction, holding you accountable – with or without access to identifying information.*[139]

The inferences gathered from the linkage of supposedly anonymous data sets can '…curtail basic ethical and political rights and liberties.'[140]

---

134 Taylor (n 28) 36.
135 ibid.
136 Suzanne Audrey and others, 'Young People's Views about Consenting to Data Linkage: Findings from the PEARL Qualitative Study' (2016) 16 BMC Medical Research Methodology 34.
137 ibid 11.
138 ibid.
139 Barocas and Nissenbaum (n 45) 51–52 (emphasis added).
140 ibid.

The extent to which 'consent' can offer meaningful respect and protection to individuals will be discussed at length below. It is appropriate to conclude here by stating that while anonymisation is clearly an important *technical* solution, it is not sufficient on its own.

3.2 The impact of the fetishisation of consent on protecting informational privacy

What is problematic with ensuring that individuals are given the opportunity to consent to the processing of their personal (or subsequently de-identified) data? Are there not many instances when there are strong practical and ethical reasons for offering individuals the opportunity to consent to a proposed use of their data? To be clear, I am *not* arguing that there is no role for consent, or that work should not continue to improve technologies that support more dynamic and informed notice and consent procedures. What I am arguing against is '*the fetishisation of consent*'[141] where the obtaining of consent is treated as *the* critical indicator of robust protection of informational privacy. Crucial to my arguments regarding the important role to be played by the public interest conditions, is understanding that the obtaining of consent is neither legally necessary nor indicative of individuals' rights and interests being respected. In fetishising consent:

> …it will be taken as axiomatic that, where there is no consent, there must be a wrong (that we do wrong if we act without consent); and, conversely, that where there is consent, there can be no wrong (that we do right if we obtain consent).[142]

This is problematic not only from an informational privacy standpoint but also for public interest uses of data. As to the latter, regardless of the public interests served by a use of data or indeed any disservice to the public interest by *not* processing data, these interests would be (and are arguably at times[143]) overlooked simply because consent cannot be obtained. The lack of consent in data processing thus becomes a signature for unethical and potentially unlawful behaviour, which as stated above, is simply not

[141] Brownsword (n 45).
[142] ibid 226.
[143] This point is considered below in relation to the failed NHS England scheme care.data.

true in a legal sense (as consent is not required under data protection law) nor, arguably, in an ethical one. This phenomenon is described by Roger Brownsword as 'consent-fetishism', or a fixation on consent where '…consent is no longer seen as an element of a larger theory of ethical or legal justification; rather, consent becomes its own free-standing justificatory standard.'[144] This is certainly evident in the research context across disciplines including biomedical research [145] and social sciences [146] where oftentimes if consent is not obtained, research is postponed and at times abandoned altogether.[147]

In the biomedical research context, a recent debacle involving the NHS demonstrates how a fixation on consent, when combined with poor public engagement and communications, can undermine potentially publicly beneficial uses of data. Here I refer to the public outcry regarding NHS England's (now failed) data sharing scheme 'care.data'. This scheme was intended to (among other things) extract data from NHS England primary care medical records unless patients opted out; these data, would in part, be used for research.[148] It is important to note that the scheme was considered to have a lawful basis via the Health and Social Care Act 2012 ('HSCA 2012') Section 259 that empowered the Health and Social Care Information Centre ('HSCIC') to require GPs and other relevant bodies to disclose to them any information deemed 'necessary

---

144 Brownsword (n 45) 226.
145 Graeme Laurie, 'Evidence of Support for Biobanking Practices' (2008) 337 BMJ; Laurie and Postan (n 39).
146 Rose Wiles and others, 'Informed Consent in Social Research: A Literature Review' (2005) NCRM 001 ESRC National Centre for Research Methods; Murphy and Dingwall (n 65); Rose Wiles and others, 'Informed Consent and the Research Process: Following Rules or Striking Balances?' (2007) 12 Sociological Research Online wiles; Sarah Dyer and David Demeritt, 'Un-Ethical Review? Why It Is Wrong to Apply the Medical Model of Research Governance to Human Geography' (2009) 33 Progress in Human Geography 46; Erdos, 'Stuck in the Thicket? Social Research under the First Data Protection Principle' (n 31); Erdos, 'Systematically Handicapped? Social Research in the Data Protection Framework' (n 31); Erdos, 'Constructing the Labyrinth: The Impact of Data Protection on the Development of "Ethical" Regulation in Social Science' (n 31).
147 In context of biomedical research: The Academy of Medical Sciences, 'Personal Data for Public Good: Using Health Information in Medical Research' (2006) 58–61 <http://www.acmedsci.ac.uk/download.php?f=file&i=13206>; In context of social sciences research Erdos, 'Systematically Handicapped? Social Research in the Data Protection Framework' (n 31); Erdos, 'Stuck in the Thicket? Social Research under the First Data Protection Principle' (n 31); Erdos, 'Constructing the Labyrinth: The Impact of Data Protection on the Development of "Ethical" Regulation in Social Science' (n 31).
148 NHS England, 'The Care.data Programme' (2016) <https://www.england.nhs.uk/ourwork/tsd/care-data/>.

or expedient' to undertake its functions.[149] This was deemed to satisfy Schedules 2 and 3 of the DPA 1998 (even if its legality could be challenged on other grounds, including, its potential incompatibility and thus violation of purpose limitation) and Section 35(1) as to disclosures required by statute.[150] It is important to clarify at this juncture that it is *not* being argued that the public interest condition as an alternative to consent (in this case or similar cases) would be a self-standing solution that fully resolves the wider issues of legality of public sector data re-use in fields other than research. As care.data illustrates, even where a public sector data reuse scheme is technically lawful per Schedule 2 and 3 of the DPA, it can clearly still fall foul of other data protection principles. The point being made here is that a significant contribution to care.data's failure stems from other (non-legal) defects inherent to the management of the scheme, namely deficient public engagement and communications.

The legal basis for processing under Schedules 2 and 3 (via the HSCA 2012) is but one area where communication to the public could have been clearer. Without such communication, the lack of consent contributed to a perception of illegality[151] and underscored the lack of 'social licence' to support the scheme.[152] Although patients could opt-out of the scheme, this was not communicated clearly to the public. As to what *was* communicated to NHS England patients:

> Information is fragmented, full of NHS jargon and neither the benefits nor the risks, nor the details of the programme have been clearly communicated to

[149] HSCA 2012, s 259. The Health and Social Care Information Centre's functions are described in Sections 254-273 of the HSCA 2012. See discussion on the legal basis for processing and specifically on the lack of consent: 'Health and Social Care Information Centre: Information Governance Assessment' (NHS Commissioning Board 2013) 3, 6 <http://content.digital.nhs.uk/media/11469/Information-governance-assessment---caredata-version-10/pdf/care.data_HSCIC_Information_Governance_Assessment_-_Feb_2013_(NIC-178106-MLSWX).pdf>.

[150] Consent was not considered to be required because of the statutory authority given by the HSCA 2012 to access the relevant data, including primary care data. This would satisfy Schedule 2 paragraph 5(b) and Schedule 3 paragraph 7(1)(b) of the DPA 1998, as the legal basis for processing required by statute. The HSCIC further considered it lawful on the basis of the DPA 1998, s 35(1) which allows disclosures required by statute. ibid.

[151] Only in terms of the legal basis for processing under Schedules 2 and 3. The plausibility of wider legal challenges (such as based on incompatible processing) are acknowledged but this is unnecessary to more fully address for this discussion.

[152] Pam Carter, Graeme T Laurie and Mary Dixon-Woods, 'The Social Licence for Research: Why Care.data Ran into Trouble' [2015] Journal of Medical Ethics.

> patients – the taxpayers who fund the NHS…The absolute crux of the issue seems to be what – exactly – you can and can't opt out of.[153]

A key justification for care.data was the potential for it to deliver various public goods, including improvements to NHS service delivery. However, this too was not explicitly communicated to the public. The scheme has since been cancelled following a UK Government review led by Dame Fiona Caldicott.[154] The public discussion which unfolded since care.data's inception, and following its recent closure, has focused on the lack of informed consent required to operate the scheme as opposed to the potential public interests served by it or the consequences of cancelling it.[155] It cannot be said that care.data failed *solely* because of the lack of informed consent sought. What it *does* show is that where public engagement and communication as to new uses of data are as deficient (as they were in this case), that the lack of consent can irreparably taint a potential public interest use of data as illegal (specifically, without a legal basis for processing). This can foreclose any discussions which might account for the full range of interests at stake, both in favour of and against the processing in question.

The fetishisation of consent is evident in far wider contexts beyond research, notably in the online and social media context.[156] Notwithstanding the implausibility of obtaining truly informed consent in modern data processing contexts,[157] the fetishisation of consent reflects the common conflation of the protection of

---

153 Olivia Solon, 'A Simple Guide to Care.data' (*Wired.co.uk*, 2014) <http://www.wired.co.uk/article/a-simple-guide-to-care-data>.
154 National Data Guardian, 'Review of Data Security, Consent and Opt-Outs' (2016) <https://www.gov.uk/government/publications/review-of-data-security-consent-and-opt-outs>; NHS England (n 148).
155 Olivia Solon, 'A Simple Guide to Care.data' (*Wired*, 7 February 2014) <http://www.wired.co.uk/article/a-simple-guide-to-care-data>; Olivia Solon, 'The Communication of Care.data to Patients Has Been an Absolute Shambles' (*Wired.co.uk*, 7 February 2014) <http://www.wired.co.uk/news/archive/2014-02/07/care-data-terrible-communication>; Eerke Bolten, 'Care.data Has Been Scrapped, but Your Health Data Could Still Be Shared' <http://theconversation.com/care-data-has-been-scrapped-but-your-health-data-could-still-be-shared-62181>.
156 Lilian Edwards and Ian Brown, 'Data Control and Social Networking: Irreconcilable Ideas?' in A Matwyshyn (ed), *Harboring Data: Information Security, Law and the Corporation* (SUP 2009); Helen Nissenbaum, 'A Contextual Approach to Privacy Online' (2011) 140 Daedalus 32; Ellen Wauters, Eva Lievens and Peggy Valcke, 'Towards a Better Protection of Social Media Users: A Legal Perspective on the Terms of Use of Social Networking Sites' (2014) 22 International Journal of Law and Information Technology 254; Custers (n 42).
157 Daniel J Solove, 'Privacy Self-Management and the Consent Dilemma' (2013) 126 Harvard Law Review 1880; Barocas and Nissenbaum, Helen (n 45); Barocas and Nissenbaum (n 45); Custers (n 42).

informational privacy with the safeguarding of autonomy. This conflation not only undermines the greater individual and social significance of informational privacy; it also detracts from the ways in which individuals' rights and interests in their data may be put at risk even where supposedly informed consent is obtained. How exactly is informed consent intended to protect an individual's informational privacy?

3.2.1 What is informed consent intended to protect and is it capable of doing so?

As the first of several alternative conditions for processing under Schedules 2 and 3 of the DPA 1998, the obtaining of consent (or 'explicit' consent if processing sensitive personal data) is one possible way data controllers can legitimise their use of personal data as 'lawful'.[158] Consent is not defined in the DPA 1998 but the DPD defines it as: '… any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.'[159] Given that the focus of this thesis is on the use and sharing of personal (or subsequently de-identified) data for *research* it is important to consider the historical origins of informed consent in that context. This brief historical detour explains the rationales underpinning the need to obtain consent in the research context. From this we can contrast the historical purpose of informed consent in relation to the context it was developed for (biomedical research) versus its modern-day manifestations in more varied data processing contexts. This exposes how consent, as it manifests in

[158] DPA 1998, Sch 1, para 1. 'Lawful' is not defined in the DPA 1998 but has been interpreted by the ICO to mean that processing is compliant with the Act and other applicable common and statutory law. To be compliant with the DPA 1998, the first data protection principle in Schedule 1, requires that a Schedule 2 condition for processing must be satisfied by the data controller (and a Schedule 3 condition if processing sensitive personal data). Therefore the obtaining of consent is one way data controllers may substantiate their legal compliance with the Act. ICO, 'Processing Personal Data Fairly and Lawfully (Principle 1)' (2016) <https://ico.org.uk/for-organisations/guide-to-data-protection/principle-1-fair-and-lawful/>.

[159] DPD, Art 2(h). However, as to sensitive personal data, Schedule 3 of the DPA 1998 requires that consent must be 'explicit'. The ICO's guidance provides that the term 'explicit' in Schedule 3 indicates '…the individual's consent should be absolutely clear. It should cover the specific processing details; the type of information (or even the specific information); the purposes of the processing; and any special aspects that may affect the individual, such as any disclosures that may be made.' Unsurprisingly, there confusion between the requirements for obtaining consent under Schedule 2 for *ordinary* personal data and Schedule 3 for *sensitive* personal data. If UK data controllers take into account the DPD's definition of consent (applicable to ordinary personal data) it is unclear what difference there is between 'explicit' versus ordinary consent. ICO, 'The Conditions for Processing' (2016) <https://ico.org.uk/for-organisations/guide-to-data-protection/conditions-for-processing/>.

modern data processing, is incapable – on its own – of effectively protecting individuals' informational privacy.

3.2.1.A The biomedical origins of informed consent

Arising out of the atrocities of Nazi research practices during the Second World War, the first principle of the Nuremberg Code provided that the obtaining of informed ('voluntary') consent was essential to conducting ethical research.[160] The obtaining of informed consent was promoted, in part, as a means to avoid the individual from being sacrificed for the greater good.[161] The importance of alerting individuals to the potential hazards of a proposed research project was central to the early development of the informed consent concept in research.[162] Under the Nuremberg Code's first principle, the essential information to be communicated when seeking consent included:

> … the nature, duration, and purpose of the experiment; the method and means by which it is to be conducted; all inconveniences and hazards reasonably to be expected; and the effects upon his health or person, which may possibly come from his participation in the experiment.[163]

Although it is not necessary for present purposes to delve more deeply into this history,[164] it is relevant to contrast the role of informed consent as it was originally developed, with the way it is understood and used today. It is necessary to consider how we progressed from the uncontroversial position where it was (and is) considered necessary to obtain informed consent in the context of biomedical research involving physical interventions, to the translation of this norm into the more varied contexts of modern data processing. What purpose does informed consent play in modern day data processing? Is it also focused on alerting individuals to potential hazards from data processing or protecting the individual from being 'sacrificed' for the greater good?

---

160 'The Nuremberg Code' para 1 <https://history.nih.gov/research/downloads/nuremberg.pdf>.
161 Heather Widdows, *The Connected Self* (1st edn, CUP 2013) 63.
162 Paul Weindling, 'The Origins of Informed Consent: The International Scientific Commission on Medical War Crimes, and the Nuremberg Code' (2001) 75 Bulletin of the History of Medicine 37, 50.
163 'The Nuremberg Code' (n 160) para 1.
164 On the historical origins of informed consent: Ruth Faden, Tom Beauchamp and Nancy King, *A History and Theory of Informed Consent* (OUP 1986); Weindling (n 162); Paul Weindling, *Nazi Medicine and the Nuremberg Trials: From Medical Warcrimes to Informed Consent* (Palgrave Macmillan UK 2004). And in the context of data protection: Eleni Kosta, *Consent in European Data Protection Law* (Martinus Nijhoff Publishers 2013) 111–129.

One potential answer to this question is provided by Ann Cavoukian, a strong advocate for enhancing notice and consent procedures online. Cavoukian describes in an idealised and somewhat unrealistic fashion, the purpose of consent:

> Consent empowers individuals to exercise additional privacy rights and freedoms, such as the ability to:
>
> - make consent conditional;
> - revoke consent;
> - deny consent for new purposes and uses;
> - be advised of the existence of personal data record-keeping systems;
> - access personal data held by others;
> - verify the accuracy and completeness of one's personal data;
> - obtain explanation(s) of the uses and disclosures of one's personal data; and
> - challenge the compliance of data users/controllers.[165]

For Cavoukian, consent plays a crucial (if not primary) role in safeguarding individuals' rights and interests in their data. She claims that the consent process contributes to the creation of 'Informed and empowered individuals [that] serve as essential checks on the uses and misuses of personal data, holding data processors accountable in a way no law, regulation or oversight authority could ever do.'[166]

At best, Cavoukian's description of consent could be characterised as idealistic. Arguably, it is an example of the unrealistic role assigned to consent in modern data processing contexts, which is ultimately harmful to the individuals concerned. It is beyond the scope of this thesis to give a more detailed treatment of the burgeoning area of research into the flaws of the informed consent model.[167] Nevertheless, it is possible to highlight the main arguments set forth against the fetishisation of consent, situate these within the appropriate theoretical context and highlight why consent is not a guarantee that individuals' rights and interests in their data will be protected. The following section does this.

---

[165] Ann Cavoukian, 'Evolving FIPPs: Proactive Approaches to Privacy, Not Privacy Paternalism', *Reforming European Data Protection Law* (Springer 2015) 297.
[166] ibid.
[167] Brownsword (n 45); Laurie and Postan (n 39); Solove (n 157); Barocas and Nissenbaum (n 45); Edward Dove and Graeme Laurie, 'Consent and Anonymisation: Beware Binary Constructions' (2015) 350 BMJ; Custers (n 42).

3.2.2 Conflating autonomy and privacy: the risks to informational privacy associated with the fetishisation of consent

Those critical of the fetishisation of consent in data protection often attribute it to a particular theory of privacy, namely 'control' based theories.[168] Control theories treat the safeguarding of the *autonomy* of individuals as the central aim of privacy; i.e. if we protect individuals' ability to make 'choices' as to uses of their personal data, we can protect their privacy. Legitimising data processing based on consent is premised on the idea that it offers data subjects a means to *control* uses of their personal data. Through the purported control this offers, individuals can 'protect' their personal data, and thus informational privacy. The presumed 'protection' offered by consent is based on several flawed assumptions, including the presupposition '…that autonomous individuals when presented with adequate information and given time to assess it will subsequently make a conscious decision whether to participate.'[169]

For the purposes of my exploration of the public interest in data protection, it is relevant to consider the inherent flaws to such theories and thus how they are problematic for the protection of individual informational privacy and broader understandings of its social value.

3.2.2.A Control based theories of privacy

Control-based theories of privacy conflate the aim of protecting privacy with the aim of safeguarding autonomy. It is useful to consider the plain meaning of both these terms. 'Autonomy' is defined in the Oxford English Dictionary as the 'liberty to follow one's will; control over one's own affairs; freedom from external influence, personal independence.'[170] Less settled is the definition of privacy which is defined as the 'state or condition of being alone, undisturbed, or free from public attention, as a matter of

---

[168] I would also include Julie Cohen's term 'privacy-as-choice' theories under this categorisation. Paul M Schwartz, 'Privacy and Democracy in Cyberspace' (1999) 52 Vanderbilt Law Review 1607; Laurie (n 28) 53–56; 69–85; Neil C Manson and Onora O'Neill, *Rethinking Informed Consent in Bioethics:* (CUP 2007) 106; Charles Raab, 'Privacy, Social Values and the Public Interest', *Politik und die Regulierung von Information* (Nomos verlagsgesellschaft, Baden-Baden 2012).

[169] Taken from Corrigan's cited discussion of 'empty-ethics' where informed consent plays a central role. Oonagh Corrigan, 'Empty Ethics: The Problem with Informed Consent' (2003) 25 Sociology of Health & Illness 768, 770.

[170] 'Autonomy', Oxford English Dictionary (3rd edition 2011).

choice or right; seclusion; freedom from interference or intrusion.'[171] This definition focuses on both the conceptual and instrumental aspects of privacy i.e. what privacy means in a substantive sense versus how one might secure or protect it. For Laurie, privacy is a *state* of being, a state of separateness from others.[172] 'Separateness' is the relevant state as opposed to being 'alone' and in this sense the definition above is inaccurate:

> *In order to be in a state of privacy there must be others from whom one can choose to be separate. This is not possible on a desert island, for one is alone.* Isolation implies a state of enforced non-access to others. Privacy, on the other hand, is a state that can easily be relaxed or maintained because it occurs in a social context. Isolation concerns the removal of individuals from that context and therefore ought not to be described as privacy.[173]

The critical point is that '…simply to be in the presence of others does not necessarily mean that privacy interests cannot be claimed.'[174] I agree with Laurie that the conceptual and more *instrumental* aspects of privacy must be distinguished, the latter which can refer to the way individuals exercise control over or otherwise protect their privacy. Certain theories of privacy focus *solely* on this instrumental aspect, neglecting the wider role and value of privacy to groups, communities and society.

Control theories of privacy focus on *individuals' choices* and thus consent to effectuate their privacy preferences. Taylor summarises the theory of 'privacy as control' where privacy 'represents control over transactions between person(s) and others, limiting or regulating access to individuals or groups, with the ultimate aim of enhancing autonomy or minimizing vulnerability.'[175] Equating the protection of privacy with the safeguarding of autonomy conflates the instrumental value with the *substance* of privacy, the latter which refers to a state of being – of an individual, group or community – in relation to 'others'. Whether and how individuals 'control' their privacy is an entirely separate matter from whether privacy does or does not exist in a particular context.

---

171 'Privacy', Oxford English Dictionary (3rd edition 2007).
172 Laurie (n 28) 6.
173 ibid 68 (emphasis added).
174 ibid.
175 Posed by Taylor in summarising Stephen Margulis' conceptualisation of privacy. Taylor (n 28) 16–17. Citing, Stephen T Margulis, 'Privacy as a Social Issue and Behavioral Concept' (2003) 59 Journal of Social Issues 243.

Laurie argues along similar lines when distinguishing between *the right* to privacy and privacy *simpliciter*.[176]

Control theories forge 'the close connection between "privacy" and "consent"' which neglects the broader public interests and social value in the protection of privacy.'[177] While it is not pertinent to delve further into debates on the different theories of privacy, it is sufficient to recognise '…that respecting the autonomy or individual liberty of an individual – allowing that individual to choose what information is given access to under what circumstances – *is no guarantee of privacy*.'[178] It is important to state that there *are* logical overlaps between privacy and autonomy;[179] in particular as to the ways in which individuals may be able to exert control or otherwise 'protect' their privacy. What is important to understand is that they are distinct concepts[180] and have different aims. Thus, we can say confidently that there is nothing problematic, in principle, about offering individuals control over uses of their personal data, such as through the opportunity to consent to such uses. What *is* problematic is that the purported 'control' given to data subjects through informed consent is neither free from external influence nor often based on enough information to provide *actual* control over the processing they are consenting to. It is the mere perception of control that is offered through the modern-day manifestation of consent to data processing. Below I more specifically consider the risks to individuals' informational privacy that are posed by the fetishisation of consent.

---

176 Laurie (n 28) 52.

177 Taylor's conceptualisation of privacy is also based on control but differs significantly from Margulis' consensus view on control theories, in that control can be exercised in many ways, such as through norms and preferences in social interactions (and thus does not rely upon control as exercised by the individual through consent). Taylor describes his theory of privacy accordingly: '…privacy is understood to represent control over transactions between person(s) and others) (rather than control over information per se), and relevant control (exercised in many different ways) can be evidenced through the norms of patterns and preferences in social interaction (rather than being understood to reside within the exercise of individual discretion)'. Taylor (n 28) 20–21.

178 ibid 20 (emphasis added).

179 Ferdinand David Schoeman, *Privacy and Social Freedom* (1st edn, CUP 1992) 20–21; Taylor (n 28) 19–22.

180 Although Taylor poses a theory of privacy which in part focuses on control, he too supports such a distinction. Taylor (n 28) 20; A distinction also supported by: Laurie (n 28) 80–85.

3.2.2.B What's the harm in asking for consent?

The efficacy of the consent transaction in data processing is legally premised on the idea that it is 'freely given specific and informed'.[181] It is helpful to consider what 'freely given' might mean. 'Freely given' in this context can be contrasted to the idea of 'freedom of choice' in markets which '…requires accurate information about choices and their consequences, and enough power-in terms of wealth, numbers, or control over resources-to have choices.'[182] To illustrate how current manifestations of consent are lacking as to these requirements, Schwartz provides a helpful illustration of the typical conditions in which consent is obtained in the online environment:

> …the act of clicking through a 'consent' screen on a Web site may be considered by some observers to be an exercise of self-reliant choice. Yet, this screen can contain boilerplate language that permits all further processing and transmission of one's personal data. Even without a consent screen, some Web sites place consent boilerplate within a 'privacy statement' on their home page or elsewhere on their site. For example, the online version of one New York newspaper states, 'By using this site, you agree to the Privacy Policy of the New York Post.' This language presents the conditions for data processing on a take-it-or-leave-it basis. It seeks to create the legal fiction that all who visit this Web site have expressed informed consent to its data processing practices.[183]

In considering such conditions (which undoubtedly will be all too familiar to the reader)[184], consent to data processing will rarely be 'freely given specific and informed'.[185] Consent is often lauded as a panacea to data protection and a means to empower individuals to take control over their personal data.[186] This view neglects the conditions in which consent is obtained. Individuals are too often stuck in what Schwartz aptly calls the 'autonomy trap'.[187] Individuals are 'locked-in' to a choice where they have surrendered their personal data '…with so little information about the uses

---

[181] DPD, Art 2(h).
[182] Julie E Cohen, 'Examined Lives: Informational Privacy and the Subject as Object' (2000) 52 Stanford Law Review 1373, 1396.
[183] Schwartz (n 168) 1661.
[184] In research, access to public services and most obviously in online, commercial contexts. Consider the NHS England care.data initiative where individual patients' data were to be used unless they exercised *opt-out* consent; the process for opting-out was not made clear nor was it clear precisely what aspects of the data initiatives patients *could* opt-out of. Solon, 'A Simple Guide to Care.data' (n 153).
[185] The often-flawed approaches taken to obtaining consent is discussed exhaustively in the literature. My thinking has been influenced, in particular, by these discussions: Brownsword (n 45); Dingwall (n 32); Laurie and Postan (n 39); Solove (n 157); Barocas and Nissenbaum (n 45); Custers (n 42).
[186] Cavoukian (n 165).
[187] Schwartz (n 168) 1662.

of personally-identified data, and their associated costs and benefits, that consent to these practices cannot plausibly be called "informed"".[188]

Thus, the harm lies not in *asking* for consent but in the false sense of comfort given by the act of asking which lulls individuals into surrendering their personal data with little understanding of what impact this can have on their informational privacy. If we consider the biomedical research underpinnings of informed consent, and the conditions in which consent is often obtained, it is clear that consent is unable to either sufficiently alert individuals to the potential hazards of data processing or to provide meaningful protection from being 'sacrificed' for far less compelling purposes than the 'greater good'.

3.2.3 Privacy and the public interest - the problem with individualistic accounts of privacy

Until now we have focused on the ineffectiveness of consent to protect individuals' informational privacy. In this section I briefly consider how the fetishisation of consent and the control based theories of privacy it relates to, is problematic to deeper understandings of the relationship between the public interest and privacy and how this impacts negatively on the protection of informational privacy. The problem I am concerned with is described by Raab in his exploration of the social value of privacy:

> The protection of privacy and the achievement of the common good or the public interest are often perceived to be poles apart as societal or policy goals. On both sides of the argument, it has become commonplace to construct the relationship between privacy and the public interest as one of zero-sum opposition: one can only increase at the expense of the other.[189]

As discussed above, the dominant approaches to data protection focus on the obtaining of consent which are most closely aligned with control-based theories of privacy. These theories view society in terms of '…relatively autonomous individuals, and holds an image of society as comprising their sum total: individuals who need

---

[188] Cohen (n 182) 1433 (emphasis added).
[189] Raab (n 168) 129; As argued by, Priscilla M Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (University of North Carolina Press 1995) 212; Similarly, Valerie M Steeves, 'Reclaiming the Social Value of Privacy', *Lessons from the identity trail : anonymity, privacy, and identity in a networked society* (OUP 2009) 193.

privacy in order to perform citizen roles in a liberal-democratic state.'[190] Autonomy focused conceptualisations of privacy construe privacy as a purely *individual* matter. An individualistic framing of privacy automatically places the rights and interests of individuals at a disadvantage when decisions are taken based on a purported balance to be struck between privacy and 'the public interest'.

Where privacy is seen as protecting only individual interests, it can be difficult to envisage many situations where the individual rights of the data subject would outweigh the wider public interest in permitting the processing of data to go ahead.[191] Simply put, the rights and interests of all of society will likely (if not always) outweigh those of one or a few individuals:

> It is all too easy for the proponents of certain public sector data processing, especially regarding surveillance and national security, to seek to down-play the importance of privacy for the community, and even to advance claims about the damage caused by privacy protection, such as 'the common good is being systematically neglected out of excessive deference to privacy'.[192]

The critical question is:[193]

'Is it possible to escape an "individual privacy v. public interest" formulation of the relationship between these two values?'

Raab suggests that one way to escape this zero-sum game is to reconceptualise privacy as a public interest itself. The value of privacy goes far beyond its meaning to the individual, serving distinct societal purposes.[194] As Raab and Bennett describe it, '…the public value of privacy has to do with its instrumental worth in underpinning democratic institutions and practices.'[195] Citing Regan's important work on the social value of privacy, privacy is considered to prevent '…the fragmentation of the public realm by allowing individuals to operate within it on the basis of their commonality

---

[190] Raab (n 168) 131.
[191] Black and Stevens (n 11) 113.
[192] ibid; Citing Raab (n 168) 135.
[193] Raab (n 168) 129 (emphasis added).
[194] Regan (n 189).
[195] Colin J Bennett and Charles Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (Ashgate 2002) 40.

rather than their differences.'[196] Thus to avoid 'the individual right of privacy [being] too often trumped by a concern for the greater social good'[197] we must recalibrate our 1) understanding of the public interest and its relationship to privacy and 2) our approach to decision-making which is intended to strike a balance between the two. To this end Taylor suggests that:

> Proper privacy protection is not simply consistent with the public interest – it is crucial to it. If privacy is a common interest, valued within a society, then it is one of the interests that public interest decision-making must be seen to take into account if decision-making processes intended to advance 'the public interest' are to retain legitimacy.[198]

Crucially, as Raab provides, such an approach requires that we expand our current understandings of the public interest to explicitly *incorporate* the protection of individual privacy rather than treat it as in opposition to it.[199] If we do so, privacy and public interests uses of data could both be supported or at least provide a 'less biased terrain for arbitrating their opposition'.[200]

It will be no surprise to the reader that I would also answer the critical question posed above ('Is it possible to escape an "individual privacy v. public interest" formulation of the relationship between these two values?'), and argue that it *is* possible. The aim of this thesis is to set forth a legally and theoretically grounded way in which policy can be shaped to overcome the current paradigms of data protection where the right to privacy is too easily sacrificed for 'the greater good'. Equally, however, I am concerned with public interest uses of data being hindered by the legal uncertainty surrounding routes to processing outwith the current consent-or-anonymise paradigm; something I consider in the section below.

---

[196] ibid 40–41; Citing: Regan (n 189) 225–227.
[197] Daniel J Solove, *Understanding Privacy* (Kindle Edition, Harvard University Press 2008) 78–79.
[198] Taylor (n 28) 32.
[199] Raab (n 168) 129.
[200] ibid 130.

4. The Consequences of the Consent-or-Anonymise Paradigm for the Undertaking of Research

Developing a clearer basis for deploying the public interest conditions supports publicly beneficial uses of data, while offering more meaningful consideration of the impact of processing on informational privacy than permitted by current approaches based on the paradigm of consent-or-anonymise. The approach developed in this thesis can help ensure that public interest uses of data are not unnecessarily hindered or abandoned for lack of a workable public interest concept. It also supports a transparent and consistent use of the public interest concept that accounts more fully for the rights and interests at stake, including the public interest in protecting informational privacy. With a better understanding of the risks posed to informational privacy, it is now appropriate to turn our attention to the impact of the consent-or-anonymise paradigm on publicly beneficial uses of data.

As indicated in Chapter 1, I am particularly interested in examining the impact of data protection law on the undertaking of social sciences and humanities research. My interest in this area arose from consultancy work and grew after my appointment as a Research Fellow to the ADRC-S project where, for the past three years, I have engaged with stakeholders (researchers, data controllers and policy makers) to understand the barriers to accessing administrative data for research in the UK. In brief, administrative data refer to *all* public-sector data collected by public authorities while carrying out their duties. Administrative data include for example, data on income tax, welfare benefits, students' exam scores, use of the health service and interactions with the criminal justice system. The problem as identified in the literature, which resonates strongly with my own experiences, is that where consent cannot be obtained or data cannot be 'sufficiently' anonymised, that research 'approval' (typically ethics approval) is significantly delayed or the project is eventually abandoned or otherwise scaled back. [201] These delays are notwithstanding those caused by the often-lengthy

[201] Julian Peto, Olivia Fletcher and Clare Gilham, 'Data Protection, Informed Consent, and Research' (2004) 328 BMJ 1029; Amy Iversen and others, 'Consent, Confidentiality, and the Data Protection Act' (2006) 332 BMJ 165; Wiles and others, 'Informed Consent and the Research Process: Following Rules or Striking Balances?' (n 146); Rose Wiles and others, 'Ethical Regulation and Visual Methods: Making Visual Research Impossible or Developing Good Practice?' (2012) 17 Sociological Research

negotiations with data controllers over access to data in the first place, negotiations stilted by the culture of caution. These delays occur even if the use of data is perfectly lawful, secure, ethical and understood to serve clearly articulated public interests. These issues arise frequently because of the insistence on obtaining informed consent.

The impracticability of obtaining informed consent for social sciences and humanities research involving population-level samples (derived from *administrative* data) illustrates the difficulty if not impossibility in such contexts, but this issue equally impacts smaller scale studies where social sciences and humanities methodologies (often qualitative) make it inappropriate (or potentially harmful to the participants) to obtain consent.[202]

Informed consent can be inappropriate[203] for the group being researched (groups and individuals involved in illegal activities[204]) or because of the setting where research is taking place (young people in a club setting[205]). As to observational and ethnographic research (which are vitally important methodologies to social sciences and the humanities), informed consent is impracticable at best since it is often impossible to inform all participants that they are being observed, especially when research is undertaken in public spaces.[206] More generally, an issue is the element of the 'unknown'

Online 8; Sethi and Laurie (n 63); Laurie and Stevens, 'Developing a Public Interest Mandate for the Governance and Use of Administrative Data in the United Kingdom' (n 63).

202 Roxanne Connelly and others, 'The Role of Administrative Data in the Big Data Revolution in Social Science Research' [2016] Social Science Research <http://www.sciencedirect.com/science/article/pii/S0049089X1630206X>; Laurie and Stevens, 'Developing a Public Interest Mandate for the Governance and Use of Administrative Data in the United Kingdom' (n 63).

203 Wiles and others, 'Informed Consent and the Research Process: Following Rules or Striking Balances?' (n 146) para 4.5.

204 In Hobbs et al, *Bouncers: Violence and Governance in the Night-time Economy*, '…using ethnography, participant observation and extensive interviews with all the main players, [the] book charts the emergence of the bouncer as one of the most graphic symbols in the iconography of post-industrial Britain.' Given the nature of the subject matter, including bouncers' working relationships with organised crime and their involvement in controlling access to drugs, it would be inappropriate and potentially dangerous during the course fieldwork to seek consent. Dick Hobbs and others, *Bouncers: Violence and Governance in the Night-Time Economy* (OUP 2003).

205 Much of the participant observation undertaken in Phil Hadfield's *Bar Wars: Contesting the Night in Contemporary British Cities* took place in a 'club' or bar setting, making the possibility of obtaining the type of consent required under data protection law both impractical and inappropriate. Phil Hadfield, *Bar Wars: Contesting the Night in Contemporary British Cities* (OUP 2006).

206 The participant observation undertaken in Hadfield's *Bar Wars* illustrates different environments that are not conducive to obtaining informed consent. His work is one example of the publicly beneficial research that can be undertaken with such methods. Similar difficulties are posed to visual image researchers: Rose Wiles and others, 'Anonymisation and Visual Images: Issues of Respect,

in social sciences and humanities research. Unlike the prescribed nature of much biomedical and clinical research, social science and humanities research does not presuppose the outcomes of a project; rather, outcomes evolve and emerge throughout.[207] This makes it particularly difficult to convey the level of information necessary for consent to be valid under data protection law. [208]

Below I will explore the ways in which publicly beneficial social sciences and humanities research is deterred, delayed, and at times abandoned altogether, due to the perceived need to obtain consent or to anonymise data. This exposes the lack of workable alternatives to consent or anonymisation to legally justify the use of personal data for social sciences and humanities research and emphasises the need for an alternative approach to data protection, namely based on the public interest.

4.1. The consent-or-anonymise paradigm at work in the social sciences and humanities context

In this section I consider the barriers posed by disparate and risk averse *interpretation* of the law by different data controllers. Most inhibitive to social sciences and humanities research is the *misperception* that consent or anonymisation are the only lawful means to access and use personal data for research, ignoring other lawful bases for processing, namely the public interest conditions. At least within the context of data protection law (as implemented in the UK), consent may be properly understood as one of several

"voice" and Protection' (2011) 15 International Journal of Social Research Methodology 41, 48. On the difficulty of obtaining consent in social sciences and humanities research generally: Wiles and others, 'Informed Consent and the Research Process: Following Rules or Striking Balances?' (n 146) para 4.5; Dyer and Demeritt (n 146) 56.

[207] Erdos considers that ' …the fluid, normative, individual and even identifiable nature of much social research ensures that it is in even profounder tension with core data protection rules than medical inquiries which are usually highly structured, generic and confidential.' Erdos, 'Stuck in the Thicket? Social Research under the First Data Protection Principle' (n 31) 134–135.

[208] In the UK, the ICO advises that an '…individual's consent should be absolutely clear. It should cover the specific processing details; the type of information (or even the specific information); the purposes of the processing; and any special aspects that may affect the individual, such as any disclosures that may be made.' If social sciences and humanities researchers cannot predict the precise outcomes of a research project, it is unlikely that any consent sought would be specific enough to satisfy this standard. ICO, 'The Conditions for Processing' (n 159).

legal grounds for processing (while acknowledging that consent may remain the default in other contexts like the law of confidence).[209]

The impact of the consent-or-anonymise paradigm is evidenced more strongly in the biomedical research context[210], but in recent years, there has been an increase in discussions on the impact of data protection law (and misperceptions of what data protection law requires) on the undertaking of social sciences and humanities research. Dingwall's discussion of the 'perverse' consequences of applying a biomedical and clinical style of regulation to social sciences research illustrates the problem under consideration here:

> At another UK university where this paper was presented, a researcher described how he had been welcomed for observational fieldwork in a large factory in an Asian country. He wanted to conclude this study by formally interviewing the plant management, but was required by his university ethics committee to obtain signed consent for this. The managers were grossly offended by the implied lack of trust and disrespect. The interviews produced meaningless data and his access to the plant was withdrawn. As he put it, a high trust society had been polluted by the low trust of the Anglo-Saxon world.[211]

Dingwall's example demonstrates how obtaining consent 'for consent's sake' can do more harm than good. Here the insistence on informed consent was detrimental to the

---

[209] For example, when it comes to accessing confidential patient information, the default is to obtain a patient's consent prior to access unless there is no other practicable alternative (referencing Section 251 of the NHS Act 2006). See discussion on the operation of Section 251 as an exception to consent here: Benedict Rumbold, Geraint Lewis and Martin Bardsley, 'Understanding Information Governance: Access to Person-Level Data in Healthcare' (Nuffield Trust 2011) <http://www.nuffieldtrust.org.uk/publications/access-person-level-data-health-care-understanding-information-governance>; Nayha Sethi and Graeme T Laurie, 'Delivering Proportionate Governance in the Era of eHealth: Making Linkage and Privacy Work Together' (2013) 13 Medical Law International 168 <http://mli.sagepub.com/content/13/2-3/168.abstract>.

[210] Strobl, Cave and Walley (n 31); Peto, Fletcher and Gilham (n 201); The Academy of Medical Sciences (n 147); Rumbold, Lewis and Bardsley (n 209) 7–8; Laurie and Sethi (n 31); Kristian Pollock, 'Procedure versus Process: Ethical Paradigms and the Conduct of Qualitative Research' (2012) 13 BMC Medical Ethics 1; Green and others (n 79) 19–20.

[211] Most of Dingwall's examples are based on experiences in the US, and illustrate the absurd results that can occur where consent is insisted upon without consideration of its merits or indeed the potential for it to cause harm in a particular context. 'A linguist seeking to study language development in a preliterate tribe was instructed by the IRB to have the subjects read and sign a consent form before the study could proceed…A political scientist who had bought a commercial mailing list of names for a survey of voting behaviour was required by the IRB to get written informed consent from the subjects before sending them the survey…An IRB attempted to deny an MA student her diploma because she did not obtain prior approval for phoning newspaper executives to request copies of printed material generally available to the public.' Dingwall (n 32) 6.

research participants (and researcher), which could have been avoided if a more context sensitive and pragmatic approach was taken. Laurie and Postan in their examination of the legal status of the consent form consider that '…the design and requirements of the clinical trials model of consent [has] become the expected ethical norm across the research spectrum."[212] Indeed, in Wiles et al review of informed consent in the social sciences, it was revealed that consent has emerged as an ethical norm for assessing the quality of such research.[213]

Even if consent is not *legally necessary* under data protection law, ethical guidelines and codes of conduct in the UK often urge researchers in the social sciences and humanities to obtain informed consent, or at least do not make clear the distinctions between the appropriate role for consent as to reuses of previously collected data versus informed consent for human participation in research (e.g. for interviews). Under the heading of 'Relationships with research participants', the British Sociological Association provides in its Statement of Ethical Practice that:

> *As far as possible participation in sociological research should be based on the freely given informed consent of those studied.* This implies a responsibility on the sociologist to explain in appropriate detail, and in terms meaningful to participants, what the research is about, who is undertaking and financing it, why it is being undertaken, and how it is to be disseminated and used.[214]

Presumably this applies to research requiring human participation as opposed to reuses of previously collected data. Nevertheless, this distinction is not made, nor is there sufficient guidance provided to researchers who *do* primarily work with previously collected datasets, as opposed to collecting data directly from individuals. While the UK's key funder of social sciences research, the Economic and Social Research Council ('ESRC') does address the issue of data reuse in its 'Framework for Research Ethics', there remains a focus on 'consent' as the basis for research (re)uses of data.[215] In a 'checklist' for researchers to consult prior to ethical review, the ESRC asks researchers

---

[212] Laurie and Postan (n 39) 18.
[213] Wiles and others, 'Informed Consent and the Research Process: Following Rules or Striking Balances?' (n 146) para 1.1.
[214] 'Statement of Ethical Practice for the British Sociological Association (March 2002)' (*British Sociological Association*, 2002) <https://www.britsoc.co.uk/equality-diversity/statement-of-ethical-practice/> (emphasis added).
[215] 'ESRC Framework for Research Ethics - Updated January 2015' (n 36) 24–25.

to consider when using 'secondary' data whether 'the consent from the primary data cover further analysis'.[216] By failing to indicate there *are* other (lawful) bases upon which reuse of data could be justified, they are implicitly prioritising consent and/or ignoring other routes to justification.

A more nuanced approach is featured in the Social Research Association's Ethical Guidelines from 2003, especially in its treatment of the relationship between informed consent and research using previously collected data.[217] The guidance not only makes clear that informed consent is *not* legally necessary under the DPA 1998 for such research, but that regardless of the permission granted by a data controller to access such data, that the focus must be on '…the likely reactions, sensitivities and interests of the subjects concerned.'[218] Here, it is made clear that assessing the impact of your research on individuals is a fundamental question of research ethics, and thus obligates a researcher whether or not informed consent can be obtained in a particular circumstance. This pragmatic approach featured in the Social Research Association's guidance is one to be applauded,[219] but numerous other social science research guidelines implicitly treat consent (or anonymisation) as the only plausible means to justify reuses of data for research; otherwise they fail to make any substantive attempt at issuing guidance on the ethics of data reuse in research as opposed to primary collection.[220]

---

216 ibid 39.
217 'Social Research Association: Ethical Guidelines' (Social Research Association 2003) 26–27, 32 <http://the-sra.org.uk/wp-content/uploads/ethics03.pdf>.
218 ibid 32.
219 Similarly see the approach to consent in: Annette Markham and Elizabeth Buchanan, 'Ethical Decision-Making and Internet Research: Recommendations from the AoIR Ethics Working Committee (Version 2.0)' (Association of Internet Researchers 2012) <https://aoir.org/reports/ethics2.pdf>.
220 'RESPECT Code of Practice for Socio-Economic Research' (2004) 2, 4 <http://www.respectproject.org/code/respect_code.pdf>; 'Code of Practice for Research: Promoting Good Practice and Preventing Misconduct' (UK Research Integrity Office 2009) para 3.7.6 <http://ukrio.org/wp-content/uploads/UKRIO-Code-of-Practice-for-Research.pdf>; Government Social Research Unit, 'GSR Professional Guidance: Ethical Assurance for Social Research in Government' (2006) 10, 13 <http://webarchive.nationalarchives.gov.uk/20150922160821/http://www.civilservice.gov.uk/wp-content/uploads/2011/09/ethics_guidance_tcm6-5782.pdf>; 'Consent for Data Sharing' (*UK Data Service*, 2012) <https://www.ukdataservice.ac.uk/manage-data/legal-ethical/consent-data-sharing>.

Applicable to both social sciences and humanities research is the Research Council's UK Policy and Guidelines on Governance of Good Research Conduct, which provides that research organisations should ensure that 'Appropriate procedures to obtain and record clearly informed consent from research participants should be in place.'[221] Research funded by the UK's Arts & Humanities Research Council ('AHRC') and ESRC must further take account of Universities UK's 'concordat to support research integrity' which characterises the lack of informed consent as a potential form of research misconduct.[222]

What is the impact of this emphasis on obtaining consent (or anonymising data) to the undertaking of social sciences and humanities research?

4.1.1 The costs of regulating social sciences and humanities research

Wiles et al[223] acknowledged the gap in empirical evidence to substantiate critiques on the regulation of social sciences research.[224] Most discussion refers to the challenges social sciences researchers face during ethical review.[225] Indeed, social sciences researchers are most often 'exposed' to data protection law through the process of ethical review within their universities. Typically, '…scrutiny of academic research usually takes the form, not of an assessment of conformity with legal rules per se, but

---

[221] RCUK, 'RCUK Policy and Guidelines on Governance of Good Research Conduct' (2015) 4 <http://www.rcuk.ac.uk/documents/reviews/grc/rcukpolicyandguidelinesongovernanceofgoodresearchpracticefebruary2013-pdf/>.

[222] 'The Concordat to Support Research Integrity' (*Universities UK*, 2012) 17 <http://www.universitiesuk.ac.uk/policy-and-analysis/reports/Pages/research-concordat.aspx>; A point echoed in: European Science Foundation, 'The European Code of Conduct for Research Integrity' (2011).

[223] Wiles and others, 'Ethical Regulation and Visual Methods: Making Visual Research Impossible or Developing Good Practice?' (n 201) para 1.7.

[224] Although most of the research discussed in this section refers to the social sciences context, in line with the AHRC's understanding of the humanities, the lack of clear boundaries between research in the arts, humanities and social sciences means that the insight gained from consideration of the latter is also arguably informative as to the former subject areas, most certainly where methods and subjects overlap: 'There is no clear boundary between the arts and humanities and many other subject areas – notably the social sciences – but a series of interfaces, and many areas of overlap. Moreover, disciplines and areas of study are continually evolving, as researchers develop new ways of approaching the study of human culture and creativity.' 'Subject Coverage' (*Arts and Humanities Research Council*) <http://www.ahrc.ac.uk/funding/research/subjectcoverage/>.

[225] Wiles and others, 'Informed Consent in Social Research: A Literature Review' (n 146); Wiles and others, 'Informed Consent and the Research Process: Following Rules or Striking Balances?' (n 146); Murphy and Dingwall (n 65); Rose Wiles and others, 'The Management of Confidentiality and Anonymity in Social Research' (2008) 11 International Journal of Social Research Methodology 417; Dingwall (n 32); Dyer and Demeritt (n 146).

of conformity with a chosen set of ethical standards which overlap with the law to a greater or lesser extent.'[226] While the aims of ethical review are broader and not focused on securing legal compliance, it seems that ethical review is becoming increasingly 'legalised' in how it is applied by university research ethics committees ('RECs').[227] This process of 'legalisation' reflects an increasing:

> …focus [by] researchers and reviewers on achieving conformity with the law, rather than taking a holistic view of the ethical context, [replacing] the process of considered ethical judgement by researchers and reviewers with an expert-based legal interpretative process, and risks displacing it with inflexible adherence to 'legal' pronouncements.[228]

The disquiet regarding the 'legalisation' of ethics review emphasises the possible ulterior motivations at work, including universities' concerns with reputation, access to research funding and legal liability,[229] as opposed to genuine ethical concerns with a proposed project.

David Erdos is one of the few scholars in the UK who has investigated the impact of the 'legal' aspects of regulating social sciences research, namely the impact of data protection law and the effect of universities' risk-averse interpretations of it which typically manifests itself during ethics review.[230] Erdos illustrates how the premises and methodological foundations of many types of social sciences research are at odds with, in particular, an insistence on obtaining informed consent:

> The obtaining of data is the lifeblood of social research. A great deal of such information is obtained indirectly whether from published material or a third party. Beyond this there may also be a need to obtain data directly from data subjects but using clearly covert or even deceptive methodologies. Such data may shed critical light on socially problematic practices which would otherwise remain hidden from view (and possible remedy). These include discriminatory attitudes on the grounds of sex, ethnicity or race, the activities and outlook of

---

[226] Charlesworth (n 32) 92.
[227] Stefan Eriksson, Anna Högland and Gert Helgesson, 'Do Ethical Guidelines Give Guidance? A Critical Examination of Eight Ethics Regulations' (2008) 17 Cambridge Quarterly of Healthcare Ethics 15; Charlesworth (n 32).
[228] Charlesworth (n 32) 92; Citing: Eriksson, Högland and Helgesson (n 227) 16.
[229] Charlesworth (n 32) 93.
[230] Erdos, 'Stuck in the Thicket? Social Research under the First Data Protection Principle' (n 31); Erdos, 'Systematically Handicapped? Social Research in the Data Protection Framework' (n 31); Erdos, 'Constructing the Labyrinth: The Impact of Data Protection on the Development of "Ethical" Regulation in Social Science' (n 31).

> members of extremist organizations, and police practices which conflict with the rule of law.[231]

Erdos references university data protection guidance for researchers where it is considered that consent 'must' be obtained for the use of sensitive personal data and where research is 'controversial' – alternative justifications for processing data are given far less credence. [232] For example, the University of Edinburgh advises that researchers should only rely upon the public interest conditions for processing sensitive personal data 'with caution'.[233] Erdos considers that universities' cautious interpretation of the first data protection principle (that processing be lawful and fair) has resulted in '…not only curtailed individual academic autonomy but, in preventing certain types of knowledge production, has inflicted a broader damage on society.'[234] Where it is not possible, or potentially harmful, to obtain consent and this is insisted upon by universities, the 'cost' is that certain forms of publicly beneficial research will simply not be undertaken.

There is no empirical 'catalogue' of social sciences or humanities research projects which have been unduly delayed or abandoned for the inability to comply with requests for informed consent or an inability to anonymise the relevant data in question (although I would hazard a guess that this is far from an *uncommon* occurrence). Anecdotally, in my own experience working with researchers in the UK, I am personally aware of *several* social sciences projects that had already received public funding but were delayed for years and at times abandoned altogether for the insistence by ethical reviewers or data controllers that they obtain informed consent or for the uncertainties surrounding *alternative* justifications for processing, namely, the public interest conditions. I have interacted with many social science and humanities researchers that have simply avoided certain topics for what they perceived would be

---

[231] Erdos, 'Stuck in the Thicket? Social Research under the First Data Protection Principle' (n 31) 142.
[232] Erdos, 'Constructing the Labyrinth: The Impact of Data Protection on the Development of "Ethical" Regulation in Social Science' (n 31) 14–15; Citing 'Research Data: Data Protection and Research' (*London School of Economics*, 2016) <http://www.lse.ac.uk/intranet/LSEServices/Legal%20Team/dataProtection/researchData.aspx>; 'Researcher's Guide to the Data Protection Principles' (*The University of Edinburgh*, 2015) <http://www.ed.ac.uk/records-management/data-protection/guidance-policies/research-and-the-data-protection-act/research/guide-principles>.
[233] 'Researcher's Guide to the Data Protection Principles' (n 232).
[234] Erdos, 'Stuck in the Thicket? Social Research under the First Data Protection Principle' (n 31) 135.

an uphill and ultimately unsuccessful battle to obtain data and ethical approval. Colleagues involved in the ADRC-S allude to the difficulties in obtaining access to administrative data where it is not practicable or possible to obtain consent:

> Access issues limit the researcher in planning their research, often prevent exploratory data analysis, and limit the extent to which new cohorts of social scientists can be trained in the use of these data. The use of secure data, which cannot necessarily be accessed by the wider research community also has implications for replication and the development of cumulative social science.[235]

Some of these issues resonate with the findings of Wiles et al who undertook a 'qualitative study of social researchers using visual methods in the UK …[to explore] the challenges they face and the practices they adopt in relation to processes of ethical review'.[236] The study revealed evidence of the consent-or-anonymise paradigm at work in ethics reviews. One participant commented: "'all ethics committees care about is anonymity and consent and if you've got a form [for study participants] to sign.'"[237] Certain researchers designed their projects in ways to *avoid* particular regulatory interactions, specifically ethical review by NHS RECs which were considered to be '…highly bureaucratic and standardised, allowing little room for variation from the norm of consent forms and anonymisation, and as being less sympathetic to qualitative research and visual methods.'[238] In summarising their findings, Wiles et al found that:

> The concern that ethics committees have about the principles of informed consent and anonymity have impacted on researchers in subtle ways such that there appears to be a reluctance among some visual researchers to make full use of their data in publications or wider communications. The consequence of ethical assessment of research may thus be to encourage conservatism in the dissemination of research findings, and what Holland et al. (2008) refer to as 'sanitised' findings.[239]

---

[235] Connelly and others (n 202) 9.
[236] Wiles and others, 'Ethical Regulation and Visual Methods: Making Visual Research Impossible or Developing Good Practice?' (n 201).
[237] ibid 3.12.
[238] ibid 3.6.
[239] ibid 4.4.

Further knock-on effects included negative impact upon the wellbeing of researchers, a shift in focus away from genuine ethical dilemmas and the curtailment of innovative research.[240]

Dingwall's scathing assessment of the situation focuses on the curtailment of social sciences and humanities research and the impact that this has on UK society.[241] He asserts that biomedical and clinical models of research governance, which are based upon the primacy of informed consent, are being imposed without regard to the different risks posed by many forms of social sciences and humanities research.[242] In contrast, Adam Hedgecoe accuses sociologists of potentially *underestimating* the risks posed by their work by over-emphasising the divide between sociological and biomedical research.[243] Hedgecoe considers the risk of harm posed by sociological research is only a difference of degree.[244] Indeed, the nature of risks posed *are* differentiated by degree, but this must be (and is not currently) reflected in *appropriate* and *context sensitive* application of regulation to different forms of research.

I am not arguing (nor do I think Dingwall is arguing) that social sciences and humanities research should be given a blanket licence to proceed without any scrutiny. Indeed, the literature exposes an overwhelming gap of evidence on the types of risk that social sciences and humanities research poses to participants, knowledge which is crucial to adequately protect informational privacy and regulate the use of data in a proportionate manner.[245] Rather, what *is* called for is a more context sensitive approach that accurately reflects the nature of risks posed but equally the public interests served

---

[240] Wiles and others, 'Ethical Regulation and Visual Methods: Making Visual Research Impossible or Developing Good Practice?' (n 201).
[241] Dingwall (n 32).
[242] ibid 3.
[243] Adam Hedgecoe, 'Research Ethics Review and the Sociological Research Relationship' (2008) 42 Sociology 873, 879.
[244] ibid.
[245] Considered by: Julie Kent and others, 'Social Science Gets the Ethics Treatment: Research Governance and Ethical Review' (2002) 7 Sociological Research Online 5.6.The lack of evidence of harm related to the use of *health* data is something my colleagues and I explored for the Nuffield Council on Bioethics and Wellcome Trust's Expert Advisory Group on Data Access. Laurie and others (n 48); Stevens and others (n 64); Kerina H Jones and others, 'The Other Side of the Coin: Harm due to the Non-Use of Health-Related Data' (2017) 97 International Journal of Medical Informatics 43.

by different types of research and the potential harms from *not* undertaking certain forms of research.[246]

Returning to Dingwall, he focuses his analysis on the regulation of social sciences and humanities research through ethics review, where consent is often insisted upon regardless of its appropriateness in a particular context. He suggests that there are at least three distinct 'costs' associated with this: 1) the curtailment of publicly funded research; 2) decreasing amounts of academic research on vulnerable and socially marginalised groups; and 3) stifled innovation with knock-on effects to the prosperity of the UK.[247] Dingwall illustrates how actual monetary costs are incurred (to the Government and thus tax payers) in reference to his and a colleague's inability to carry out a piece of publicly funded research due to the need to obtain approval from 350 NHS hospitals 'potentially generating about 1600 signatures and 9000 pages of documentation'.[248] As a result of this, they could not deliver on the original aims of the research and instead completed a significantly limited piece of work. It is worthwhile noting that this research (as originally commissioned) was to investigate harms arising out of the reuse of single-use devices in healthcare, which at the time was thought to lead to approximately seven deaths per year and several post-operative infections.[249]

From this analysis, it is clear that we need even more evidence of the ways in which the consent-or-anonymise paradigm negatively impacts upon the undertaking of publicly beneficial research. Such evidence could support a more *proportionate* and context-sensitive approach to 'regulating' social sciences and humanities research. With an empirical catalogue of 'impact' on publicly beneficial uses of data, a sense of urgency could be created to persuade policy makers that the UK needs alternative approaches to data protection outwith the current consent-or-anonymise paradigm.

---

[246] Myself and colleagues have considered the potential 'harms' from not using data where it may be in the public interest to do so. Jones and others (n 245).
[247] Dingwall (n 32) 9–10.
[248] ibid 11.
[249] ibid 10.

5. Moving Beyond Consent or Anonymisation

In examining the predominance of the consent-or-anonymise paradigm, and the lack of meaningful engagement with the public interest conditions, it becomes clear that this is an underexplored area of data protection. Neither data protection law nor subsequent guidance has provided a clear basis for deploying the public interest conditions. The consent-or-anonymise paradigm is detrimental to both the protection of informational privacy *and* to publicly beneficial uses of data.

Social value theories of privacy conceptualise privacy as serving a distinct and valuable public interest. Such understandings of privacy do not only focus on the benefits conferred on specific individuals, but also on the broader societal benefits gained from ensuring that privacy is protected. There is indeed a distinct and valuable public interest in protecting the informational privacy of individuals. Understanding the protection of informational privacy as a discrete public interest allows for the development of approaches to data protection which do not automatically create antagonistic relationships between the protection of individuals' rights and interests in their data against those of society which may favour the use of data to achieve socially beneficial outcomes.

The public interest is at stake both in the use and protection of personal data. It is with this more cooperative conceptualisation that I consider in subsequent chapters the role the public interest concept can play in new approaches to data protection which offer more transparent, dynamic and fairer resolution of the tensions between the protection and use of personal data. However, to successfully implement the public interest concept in a *legal* context, we must first establish a legitimate legal basis for doing so. In Chapter 3, through extensive analysis of the legislative history to the DPA 1998 and DPD, I consider the reasoning behind the inclusion of the public interest conditions. Through this analysis I expose the relevant legal contours that must be respected when deploying the concept in practice.

Chapter 3 Tracing the History and Application of the Public Interest in Data Protection Law – a UK and European perspective

1. Introduction

The underlying aim of this thesis is to develop a new understanding of the public interest concept in data protection and to suggest a new approach to resolving the tensions between the protection of informational privacy and use of personal data. As discussed in Chapter 2, the consent-or-anonymise paradigm not only hinders the undertaking of publicly beneficial research but more broadly represents a flawed, albeit common, approach to data protection. This is incapable of ensuring individuals' rights and interests in their data are fully accounted for. It is equally unable to ensure that public interest uses of data are facilitated. In this broader sense, the consent-or-anonymise paradigm detracts from the dual public interests underpinning European and thus UK data protection law which is to promote *both* the use and protection of personal data.

As briefly referenced in Chapter 1, it is important to highlight the dearth of understanding on the public interest conditions in data protection and the consequent need for this new approach. The public interest concept is not defined in either the DPD or DPA 1998. In the context of privacy injunctions and the media, Mr Justice Eady explained that:

> A decision on public interest must be capable of being tested by objectively recognised criteria. But it could be argued as a matter of policy that allowance should be made for a decision reached which falls within a range of reasonably possible conclusions.[250]

[250] *Mosley v News Group Newspapers Ltd* [2008] EWHC 1777 (QB) [138]. Gillian Black, *Publicity Rights and Image: Exploitation and Legal Control* (Hart Publishing Ltd 2011) 173.

Without a legal definition or interpretation within subsequent and authoritative guidance, such 'objectively recognised' criteria are lacking within the data protection context. The ICO has attempted to unpack the application of the public interest concept[251] to section 32 of the DPA 1998, which exempts processing for the 'special purposes' of journalism, literature and art from several provisions of the Act[252], if (among other requirements) the data controller '...reasonably believes that, having regard in particular to the special importance of the public interest in freedom of expression, publication would be in the public interest.'[253] This guidance was developed specifically for interpreting section 32 and therefore cannot be directly applied to the public interest conditions; indeed there is no precedent to suggest this is, or would be appropriate (not least because the public interest conditions apply to a far broader range of processing). The existence of this guidance does, however, indicate the *possibility* of producing something similar on the public interest conditions.

Given the absence of any such guidance or critical analysis on the public interest conditions in data protection literature, there is a fundamental lack of understanding as to the potential 'range of reasonably possible conclusions' which could lead to justifiable reliance on the conditions. The purpose of this chapter is to begin the task of unpacking the intended role and scope of the public interest conditions by tracing the reasons for its inclusion in the legislation. With this relevant historical and legislative grounding, a new approach to understanding and resolving the public interests in data protection can be developed.

As the guiding instrument of data protection law in Europe, I first analyse the legislative history to the DPD, focusing on the discussions surrounding the inclusion of the public interest provisions. Although the legislative history clarifies the statutory role of the public interest provisions, uncertainty remains as to the substantive meaning

---

[251] ICO, 'Data Protection and Journalism: A Guide for the Media' (2014) 32–34 <https://ico.org.uk/media/1552/data-protection-and-journalism-media-guidance.pdf>.
[252] Comparing the breadth of exemptions available for journalism, literature and the arts versus those applicable to 'research purposes', David Erdos argues that academic research *should* be able to avail of the section 32 exemptions as opposed to the more limited exemptions available for research under section 33. David Erdos, 'Freedom of Expression Turned on Its Head? Academic Social Research and Journalism in the European Union's Privacy Framework' [2013] Public Law 52.
[253] DPA 1998, s 32(1).

of the public interest concept. To this end, in the second part of the chapter, I consider the UK's implementation of the public interest provisions into the DPA 1998 to assess the extent to which these uncertainties are resolved. The chapter concludes by outlining what is 'known' and 'not known' as to the public interest provisions in the DPD and DPA 1998; the purpose and relevant procedure defining the scope for the provisions are known but the crucial public interest threshold and what it means to be 'in the public interest' remains undefined and unsubstantiated, a point to be addressed in forthcoming chapters.

2. The Legislative History to the DPD: The Intended Role and Scope of the Public Interest Concept

A logical first step to developing an understanding of the intended role and scope of the public interest provisions in European data protection law is to examine the reasons *why* legislators included the public interest concept in the first place and what *their* understanding of the term was at the time the legislation was being drafted. Although the geographical focus of this thesis is the UK in the main, given the guiding force of the DPD and its role in interpreting *national* implementing legislation,[254] I consider the legislative history to the Directive first (the *travaux préparatoires* or in short form the *travaux*). Below I track the evolution of the public interest concept and its inclusion in relevant provisions from its introduction into the draft Directive until its final and enacted form.[255]

As to my methodology, I first identified the sources of key material. This included documentation relating to each procedural step in drafting the DPD. Although some of the *travaux* was available on the *Eur-LEX* website, many documents were not.[256] This required further investigation on the public register of the *Council of the European*

---

[254] In the UK under the authority of *HP Bulmer Ltd v J Bollinger SA*, Lord Denning held that in relation to laws enacted based on EU legislation (such as the DPA 1998), interpretation must not be confined to the 'English text' but to consider the intentions of the framers of the European instrument. [1974] EWCA Civ 14, [1974] Ch 401 [426].
[255] A timeline of the *travaux préparatoires* to the DPD may be found here: 'EUR-Lex - 1990_287 - EN' (*EUR-Lex: Access to European Union law*) <http://eur-lex.europa.eu/procedure/EN/100979>.
[256] ibid.

Union[257] containing 'all non-sensitive documents submitted to the Council or to one of its preparatory bodies which are to serve as a basis for deliberations, could influence the decision making process or reflect the progress made on a given subject'.[258] When it became clear that not all the *travaux* were available online, I made a freedom of information request per Regulation (EC) No 1049/2001 regarding public access to European Parliament, Council and Commission documents.[259] In combining these sources, I searched each document (over 1,300 pages) for any mention of 1) 'public interest', 2) any analogous terms e.g. 'general interest' and 3) 'research'. This analysis would unearth previously overlooked discussions regarding the public interest concept in data protection law and the role of the public interest provisions, especially in relation to research.

2.1 1990 proposal for a Council Directive on the processing of personal data

The DPD was preceded by the introduction of international provisions on the legal protections and principles of data protection. These included the 1980 Organisation for Economic Development's ('OECD') Privacy Guidelines[260] and the 1981 Council of Europe 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' ('Convention 108').[261] Convention 108 arose out of 'the threat to individual privacy posed by computerisation; and the desire to maintain a free flow of information between trading nations.'[262] To accede to the Convention a State

---

257 'Search in the Register' (*European Council, Council of the European Union*) <http://www.consilium.europa.eu/register/en/content/int/?typ=ADV&lang=EN>.
258 From the email response to my freedom of information request to the General Secretariat of the Council of the European Union.
259 I am grateful to David Erdos for also sharing the *travaux* documents he obtained for his article Erdos, 'Freedom of Expression Turned on Its Head? Academic Social Research and Journalism in the European Union's Privacy Framework' (n 252).
260 'OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data - OECD' (as updated in 2013) <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>.
261 Though beyond this discussion, it is important to recognise the role of Convention 108 in being the first international instrument to establish the protection of personal data as a separate right when adopted by the Council of Europe in 1981. Currently there are 48 signatories to the Convention. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ET 108 1981.
262 Ian Walden, 'Privacy and Data Protection', *Computer Law: The Law and Regulation of Information Technology* (7th edn, OUP 2011) 575.

would need to enact national data protection legislation, which the UK fulfilled with the Data Protection Act 1984 ('1984 Act'). It is beyond the scope of this thesis to provide any in-depth analysis of the 1984 Act; I focus solely on the current state of the law which is based upon the DPD to be amended yet again in 2018 when the GDPR comes into force (although it remains unclear the extent to which UK data protection law will continue to fully align itself with the Regulation post-Brexit). For present purposes, it is enough to acknowledge that the 1984 Act was the *first* data protection legislation in the UK which remained in force until the passage of the DPA 1998.[263] This and other national data protection legislation enacted for the purposes of acceding to the Convention diverged greatly and thus the Convention was unable to attain consistency in application and implementation by signatory states.[264] To achieve this uniformity in protection and, furthermore, to secure the development of the internal market in Europe, the European Commission submitted a 'Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data' ('1990 Proposal') in July 1990.[265]

It is not necessary to examine the entirety of the 1990 Proposal and all successive amendments made therein. Of primary relevance to this discussion is the introduction of the 'public interest' concept into the legislation, especially in its iteration as a legal justification to process (ordinary) personal data and sensitive personal data. Although Convention 108 and the OECD Privacy Guidelines both allow for derogations based on various public policy grounds (*ordre public*),[266] the later drafts of the DPD introduced

---

[263] In contrast with the DPA 1998, the 1984 Act only applied to the *automatic* (electronic) processing of data and not to manual records. 1984 Act, Pt 1, s 1(2).

[264] Discussed in the *travaux* as a key reason for introducing the Draft DPD: 'The abovementioned Council of Europe Convention has not led to a reduction in this diversity because, firstly, it leaves open a large number of options as far as implementation of its basic principles is concerned, and secondly, it has been ratified by only seven Member States (Denmark, France, Germany, Ireland, Spain and the United Kingdom), of which one (Spain) still has no domestic legislation.' European Commission, 'Commission Communication on the protection of individuals in relation to the processing of personal data in the Community and Information Security: Explanatory Memorandum' (13 September 1990) SYN 287, 15. (Unless a website is provided, all references to the *travaux* are held on file.)

[265] 'Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data 1990/C/277/03' <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:1990:277:FULL&from=en> (hereinafter '1990 proposal').

[266] OECD Guidelines (n8), Paragraph 4 'Exceptions to the Guidelines'; Convention 108 (n9), Art 9(2)(a).

the public interest concept for the first time into data protection legislation. On this point, the legal grounds for processing personal data were more limited and structured differently under the original 1990 Proposal than in the finalised and current DPD, but were not necessarily negative for research processing.

The lawful grounds for processing under the 1990 Proposal were divided between those applicable to public sector bodies and private sector entities.[267] As to public bodies, the 1990 Proposal makes a distinction between the lawful grounds for the 'creation or any other processing of personal data' and treats separately 'the communication' of personal data held by public bodies. As to the former category, the creation of files 'or any other processing' by a public sector body would be lawful if it was necessary for that public body to perform their tasks. Processing for any other purposes would only be lawful if 1) the data subject consented; 2) the processing was based on a further legal obligation; 3) the legitimate interests of the data subject did not preclude this further processing, or 4) the further processing was necessary to '… ward off an imminent threat to public order or a serious infringement of the rights of others.'[268] As to the *communication* of personal data held by a public authority, more limited grounds were set forth such that it would be lawful only if it was 1) necessary for the public body to perform their tasks or 2) 'requested by a natural or legal person in the private sector who invokes a legitimate interest, on condition that the interest of the data subject does not prevail.'[269]

As to the processing of data by private sector entities, the grounds for processing were more limited. Processing by a private sector entity would need to be based on consent; if consent was not possible only three other grounds were provided: 1) that processing was required to carry out a contract; 2) that data were publicly accessible and used solely for correspondence; or 3) that the processing was in the legitimate interests of the controller 'on condition that the interest of the data subject does not prevail.'[270]

---

[267] Articles 5-6 dealt with the grounds for processing data by public sector bodies, while Article 8 dealt with the grounds applicable to private sector bodies.
[268] 1990 Proposal, Art 5(1).
[269] 1990 Proposal, Art 6.
[270] 1990 Proposal, Art 8.

The 1990 Proposal did *not* include a legal ground for the processing of personal data (for either public sector or private sector bodies) on the basis that it is in the public interest (although Article 8 of the Proposal does allow Member States to derogate further processing conditions).[271] Article 17 did provide that Member States may for reasons of 'important public interest' allow the processing of special categories of personal data.[272] The terminology 'important public interest' is not further defined in the 1990 Proposal, however Recital 16 elucidated that reasons of important public interest notably include those 'in relation to the medical profession'.[273]

Given that research is the primary example of data processing referred to throughout this thesis, it is worth noting that the 1990 Proposal did not make special provisions for research. However, it is possible that the mention of 'the medical profession' in Recital 16 may have been an early recognition of the importance of *medical* research and the use of personal data for such endeavours.[274] Moreover, if considering the reuse of public sector data for *research*, the grounds for processing ordinary personal data in the 1990 Proposal would allow this if 'the legitimate interests of the data subject did not preclude' the research use in question. In combination with Article 17 and the potential for Member States to enact derogations for special categories of personal data, there were ways in which both ordinary and special categories of personal data could be processed for research. What is important to note is that even at this early point in the DPD's history, Recital 16 and Article 17 demonstrated Member States' concern that certain forms of data processing may not always be capable of satisfying other legal conditions such as 'consent' and may require justification on the basis of a particular public interest served.

---

[271] The 1990 Proposal did not have the equivalent of the DPD's Article 7(e) (i.e. 'processing is necessary for the performance of a task carried out in the public interest').
[272] Understood in the UK as 'sensitive' personal data.
[273] 1990 Proposal, Recital 16.
[274] Although at this stage there are also exemptions made for freedom of expression and the press (albeit without explicit mention of the 'public interest' served by these) ibid Art 19.

2.2 1991 opinion on the proposal for a Council Directive on the processing of personal data

In response to the 1990 Proposal, the European Council consulted with the Economic and Social Committee ('ESC') in accordance with usual procedures for the drafting process,[275] which subsequently provided its opinion on the draft Directive.[276] In relation to the 'public interest', they approved the notion of Member States derogating from the prohibition of processing special categories of personal data, such as for 'important public interest' grounds (Article 17), so long as such derogations were subject to 'specific regulations' which at the time, they did not elaborate on further.[277]

This presents the first of many inconsistencies in the treatment of the public interest concept in the draft Directive. Here the inclusion of 'important' before 'public interest' seems to suggest the prospect that there are *unimportant* public interests. However, more to the point is that the ESC found the legal grounds provided in the 1990 Proposal inadequate: 'The Directive goes further than Convention 108[278] by seeking to establish criteria for deciding whether processing is lawful. These criteria appear inadequate or open to differing interpretations'.[279] The use of vague terms, such as 'legitimate interests', without further explanation, was considered (even at this early stage) problematic[280] and is indicative of a desire to create legislation that rejects such ambiguity. Curiously, however, the use of equally vague terms such as 'important public interest' was *not* commented on regarding the processing of special categories of personal data. Overall, the ESC's 1991 Opinion cements the idea that processing for reasons in the public interest *should* be allowed (at least for special categories of personal

---

[275] 'Legislative Powers: Ordinary Legislative Procedure' (*European Parliament: About Parliament*) <http://www.europarl.europa.eu/aboutparliament/en/20150201PVL00004/Legislative-powers>.
[276] 'Opinion on: — the Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data, — the Proposal for a Council Directive Concerning the Protection of Personal Data and Privacy in the Context of Public Digital Telecommunications Networks, in Particular the Integrated Services Digital Network (ISDN) and Public Digital Mobile Networks, and — the Proposal for a Council Decision in the Field of Information Security' (Economic and Social Committee 1991) C 159/38 <http://publications.europa.eu/resource/cellar/4ed85510-f142-461b-bd0d-fc850f77fbf3.0004.01/DOC_1> (hereinafter '1991 Opinion').
[277] 1991 Opinion, 43.
[278] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ET 108 (n 261).
[279] 1991 Opinion, 41.
[280] ibid.

data and if 'important'), if suitable (but as yet unspecified) safeguards for said processing were in place.

2.3 1992 first reading of the European Parliament

The DPD continued to evolve after the first reading of the European Parliament ('First Reading of the European Parliament') where significant amendments were made to the draft Directive.[281] The amendments represented, at times, a stricter stance on the protection of personal data than the original 1990 Proposal. Importantly, Parliament completely removed the provisions allowing the lawful processing of special categories of personal data on the basis of 'important public interest' grounds.[282] In its place, Parliament proposed a complete ban on the processing of special categories of personal data by the private sector: 'The Member States shall provide in their law for a ban on the processing of data of a strictly private nature in the private sector.'[283] No similar ban was made for *public* sector data controllers.

The term 'public interest' is in fact entirely removed from the First Reading of the European Parliament. However, the public interest may have been introduced in a less explicit way through the amendments to Article 8(2) which covers the legal grounds for the 'communication' or reuse of ordinary personal data from a data controller to third parties. Article 8(2)(g) provides that a data controller may reuse personal data after collection:

> insofar as it is necessary to safeguard the legitimate interests of a third party *or the general public*, provided that the interests of the data subject that warrant protection are not harmed.[284]

---

[281] European Parliament, 'Position of the European Parliament on Proposal for a Directive I COM (90) — C3-0323/90 — SYN 287/Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data, 11 March 1992 (First Reading)' (1992) OJ C94/173 <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOC_1992_094_R_0063_01&from=EN> (hereinafter 'First Reading of the European Parliament'). Explanatory notes available here: <http://aei.pitt.edu/10375/1/10375.pdf >.

[282] First Reading of the European Parliament, Amendment No 63, Art 17(2).

[283] Here special categories of personal data were referred to as 'data of a strictly private nature'. ibid Amendment No 63, Art 17(2).

[284] ibid Amendment No 32, Art 8(2) para (g) (emphasis added).

Here the safeguarding of the legitimate interests of the 'general public' could be interpreted as an iteration of the public interest concept, representing a predecessor provision to the later inclusion of a standalone legal ground on the basis of the public interest. More likely, however, is that this provision represents a precursor and combination of *both* the public interest provision in the finalised Article 7(e) and the legitimate interests provision in Article 7(f).[285]

Continuing with the analysis of Parliament's Article 8(2)(g), the reuse of personal data is allowed in the interests of 'the general public' *so long as* the interests of individual data subjects are not harmed (the latter are not defined but presumably include their interests in privacy). This does not indicate that a balance may be struck between the interests of the general public and of the individual. Rather a stricter approach is required – if *any* harm would result from the 'communication' or reuse of data, reliance on this provision would become invalidated. Thus, and unlike the finalised public interest provisions in the DPD, considerations of harm to the data subject are explicitly required when considering justification for the reuse of personal data on this basis. However, as per the finalised DPD, the understanding of harm in the context of data protection is indeed a narrow one, equated with tangible harms causally connected to financial 'damages'.[286] This is despite the clear intention expressed by the European Commission, in its original communication on the DPD, that harm was intended to be broadly interpreted as including non-physical as well as physical damage.[287]

The stricter approach taken by the European Parliament to regulating the processing of special categories of personal data, is juxtaposed by the apparent leniency granted to data controllers elsewhere within the draft Directive, for example, in the inclusion of new and broader legal grounds for processing personal data that were not in the

[285] In the final version of the DPD, Art 7(f) omits any mention of 'the general public' and instead merely refers to the safeguarding of the data controller's legitimate interests. If safeguarding the interests of 'the general public' are indeed synonymous with the notion of the public interest, it is contended here that this was subsequently separated into a standalone legal basis in Art 7(e).
[286] 'Damages' are referred to but not elaborated upon in this iteration of the draft Directive. First Reading of the European Parliament, Recital 20 and Art 21.
[287] European Commission, 'Commission communication on the protection of individuals in relation to the processing of personal data in the Community and Information security' (1990) COM 90 314 final 40 <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:51990DC0314&from=EN>.

original 1990 Proposal. For instance, consider the addition of a legal ground which would have allowed data controllers to process personal data (for any reason) so long as 'the data subject has been given an opportunity to object to the processing and has not done so'.[288] Why would a data controller obtain consent if an even lesser standard than opt-out would suffice? Further, consider the amendments in Article 8(2)(i) which would legitimise the reuse of personal data 'for research and statistical purposes on condition that the personal data is depersonalized'.[289] While an interesting evolution of the DPD as a whole, the amendments proposed by the European Parliament do not further our understanding of the public interest concept and its intended role and scope for data protection; indeed they remove explicit use of this term from their version of the draft Directive.

2.4 1992 European Commission compromise draft of the Directive

Taking into account the First Reading of the European Parliament, the European Commission adopted a compromise version of the proposed Directive in October 1992 ('1992 Compromise Draft').[290] The 1992 Compromise Draft reinstated the 1990 Proposal's Article 17 (grounds for processing special categories of personal data), into Article 8. The revised Article 8 restored several exceptions to the prohibition on processing special categories of personal data including reinstating a legal basis for processing based on 'important public interest grounds'.[291] In the explanatory memorandum to the 1992 Compromise Draft, the Commission seemed to indicate that the legal basis for processing on grounds of 'important public interest' should be given *substance*, as seen by their attempt to add context to this vague provision:

> Paragraph 3 reproduces Article 17(2) of the initial proposal, permitting exemptions on 'important public interest grounds.' An exemption should be given, for example, to international human rights organizations which require such data for their work, provided they can offer suitable safeguards.[292]

---

[288] ibid Amendment No 30, Art 8(1)(ca)(new).
[289] First Reading of the European Parliament, Amendment No 32, Art 8(2)(i).
[290] European Commission, 'Amended Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data' (1992) OJ C311/30 <http://aei.pitt.edu/10375/1/10375.pdf> (hereinafter '1992 Compromise Draft').
[291] 1992 Compromise Draft, Art 8(3).
[292] ibid Explanatory Memorandum, 18.

This attempt to provide substance to the concept of the public interest is underwhelming. The explanatory memorandum provides only one example on what an important public interest may be aside from the mention of processing data related to the medical profession in their amended Recital 17.[293] Thus, while the Commission implies their desire to *avoid* the use of ambiguous terminology in the Directive, no further explanation is provided as to what may be considered an important public interest for the purposes of the legislation or indeed what criteria might be used to assess the public interest in processing in each case.

Not only does the Commission reinstate the 'important public interest' ground for processing special categories of personal data in the 1992 Compromise Draft, it goes further and introduces a separate legal ground for processing ordinary personal data based on the public interest. This is essentially the same as what is currently in the DPD, Article 7(e):

> processing is necessary for the performance of a task in the public interest or carried out in the exercise of authority vested in the controller or in a third party to whom the data are disclosed.[294]

With the addition of this new public interest ground for processing ordinary personal data (and the complete reformulation of other legal grounds to processing without consent)[295] the Commission makes clear that: 'Consent is no longer the main criterion, subject to exceptions; *it is now the first of several alternatives*.'[296] This is crucial as it rejects the primacy of consent and reflects a far more balanced and proportionate approach to the concept of lawful processing.

---

[293] ibid Recital 17.
[294] 1992 Compromise Draft, Art 7(e) which is nearly identical to Art 7(e) in the current DPD bar certain grammatical changes i.e. the final version of the DPD includes the words 'carried out' prior to the words 'in the public interest'.
[295] The 1992 Compromise Draft significantly modified the original 1990 Proposal's legal grounds for processing, which were found in Articles 5, 6 and 8. The 1992 Compromise Draft combined all the legal grounds into a single Article 7 (mimicking the format we are familiar with under the current DPD). The legal grounds added in 1992 included processing necessary: for a contract (Art 7(b)); for compliance with a legal obligation (Art 7(c)); to protect the vital interests of the data subject (Art 7 (d)); for a task in the public interest (Art 7(e)); and for the legitimate interests of the controller or third party (Art 7(f)).
[296] 1992 Compromise Draft, Explanatory Memorandum, 16 (emphasis added).

With specific regard to the public interest ground for processing, the Commission states that: 'The same applies to the new Article 7(e)'. A reference is then made to their previous statement that: 'The reference to processing in order to comply with an obligation imposed by national or Community law *has been maintained* (new Article 7(c))'.[297] This would mean that the Commission's addition of a standalone public interest ground to processing was in fact considered a mere *transposition* of what was previously in the 1990 Proposal, even though the term 'public interest' was not used in relation to the processing of ordinary personal data. Although the Commission did not explicitly say, it is likely they were referencing Article 5(b) of the 1990 Proposal which, in pertinent part provided:

> …the creation of a file and any other processing of personal data shall be lawful in so far as they *are necessary for the performance of the tasks of the public authority in control of the file*'.
>
> …it is necessary in order *to ward off an imminent threat to public order* or a serious infringement of the rights of others.[298]

On this reasoning, in 1992 Article 7(e) was considered limited to processing by public authorities in the performance of their tasks or 'to ward off an imminent threat to public order', suggesting a rather high threshold for processing to be considered in the public interest. However, the plausibility of this restrictive interpretation can be quickly dismissed. First, Article 7(e) cannot be limited to public authorities given that it distinguishes between processing that is necessary: 1) 'for the performance of a task in the public interest'; 2) 'carried out in the exercise of public authority vested in the controller'; or 3) 'in a third party to whom the data are disclosed'.[299] Second, it is clear from Recital 17 (at least in regards to processing special categories of personal data) that the public interest can encapsulate far less pressing matters, such as those related to the medical profession, not merely 'imminent threats to public order'.

This is simply to say that the Commission's 1992 Compromise Draft does not help advance any further understanding of what precisely a task 'in the public interest' might

---

[297] ibid 17 (emphasis added).
[298] Compare Art 5 of the 1990 Proposal to Art 7(e) of the 1992 Compromise Draft (emphasis added).
[299] 1992 Compromise Draft, Art 7(e) (emphasis added).

be in the context of the myriad of possible purposes for data processing. Aside from the three examples mentioned (processing related to the medical profession, by human rights organisations and to ward off imminent threats to public order), no other examples or objective criteria are given to explain what may be considered sufficiently in the public interest or as an 'important' public interest in terms of data processing more generally. Interestingly however, the three examples provided *do* have some conceptual similarities in that they represent circumstances where consent may be impossible or impracticable to obtain and 'the public interest' nevertheless requires certain processing of personal data e.g. if a patient is critically injured, if a human rights organisation is providing aid in a war-torn country or if a sudden and severe threat to public safety arises.

2.5 1993-1994 Council of the European Union readings of the 1992 compromise draft

The addition of Article 7(e) in the 1992 Compromise Draft was noticeably broader than the 'equivalent' provisions in the 1990 Proposal as public interest terminology presumably is used to encompass a wider range of processing scenarios, rather than previous and implicit references to processing within other legal grounds which may have a mere 'flavour' of the public interest.[300] Further consideration of the 1992 Compromise Draft, reveals Member State reactions to the addition of a standalone public interest ground for processing in the new Article 7(e).[301] For example, from the first reading of Articles 1-7 by the Working Party on Economic Questions, France wanted to make clear 'the distinction to be made between "a task in the public interest" and "the exercise of public authority"', given the notably broader scope of Article 7(e) than the processing encompassed by Article 5(b) of the 1990 Proposal (limited to the performance of the tasks of a public authority).[302] If there would be two separate grounds, one limited to the actions of public authorities, and one with regard to

[300] Article 5(b) of the 1990 Proposal, only covers specific data processing scenarios which may be in the public interest, including data processing by a public authority or processing that 'is necessary in order to ward off an imminent threat to public order or a serious infringement of the rights of others.'
[301] Council of the European Onion, 'Outcome of Proceedings of: Working Party on Economic Questions (Data Protection) on 5 and 6 October 1992' 9388/92 ('Outcome of Proceedings 9388/92'.
[302] ibid 20.

processing in the public interest, there presumably would be a difference between the two but this distinction was as yet unclear.

This uncertainty is shared and evidenced by Germany's request for specific examples of what tasks in the public interest would be covered over and above those cases, that would fall under Article 7(c) which encompasses processing undertaken to comply with an obligation under EU or national law.[303] Here, we again see a request to clarify what precisely the 'public interest' means if it is to be distinguished from other acts by the State or arising from legal obligations. Specific examples of 'tasks' in the public interest would *eventually* be provided in Recital 34 of the finalised DPD, which would include, for example, scientific research. However, these were *not* included in the Compromise Draft under consideration. Thus, it was left entirely unclear exactly what type of processing may be considered in the public interest. During the period between 1992-1994, the *travaux* reveals Member States lobbying efforts to exclude or create exemptions for certain forms of processing, some of which are later included as 'public interest' examples in Recital 34.

The lobbying which took place during this time represents inconsistencies in the treatment of the public interest as a concept and moreover, a lack of engagement with its substantive meaning. At no time did Member States or European legislators suggest or introduce criteria to assess the public interest in processing; descriptive examples are all that is ever provided. Below I examine the specific lobbying efforts of Member States in this regard, which demonstrates the lack of reasoning behind the eventual inclusion of certain forms of processing as examples of the public interest. This reveals the *political* role of the 'public interest' justifications for processing as a potential compromise for Member States who desired complete exemption from the scope of the DPD for certain processing activities. Rather, Member States 'received' lesser restrictions in the form of an alternative justification for processing without obtaining informed consent.

---

[303] Outcome of Proceedings 9388/92, 19-20.

2.6 Member States' lobbying and the public interest

During the remaining drafting process, various Member States lobbied for specific processing activities to be excluded or exempted under certain circumstances, from the scope of the proposed Directive. Many of these activities were eventually recognised as processing in the 'public interest' in Recital 34[304] and justifiable on that basis as provided for in Articles 7(e) and 8(4)[305] of the DPD. Before considering the specific types of processing lobbied for, noting especially those which were eventually categorised as 'in the public interest', it is important to consider the logic behind these lobbying efforts. As stated above, soon after the inclusion of the public interest justifications for processing ordinary and special categories of personal data, Member States, (for example, France, Germany and Greece), expressed confusion and uncertainty regarding the scope of the public interest concept.[306]

Most of these concerns, and similar discussions recorded in the *travaux*, were focused on the public interest as a justification for the processing of *special categories* of personal data (i.e. in Article 8(4)). This is because the public interest justification for processing special categories of personal data was offered as a compromise to Member States who were concerned that certain forms of processing which required such data (for example, health data[307] and trade union membership[308]) would be impeded if consent was required. It is interesting to note that early in these discussions (in October 1992), the Commission admitted defeat in their attempts to define the concept; as stated in a footnote, they 'remained open to suggestions, although felt it difficult to clarify this notion further.'[309]

Indeed, as the remaining *travaux* reveal (and as evidenced in the final text of the DPD), legislators were seemingly guided *entirely* by Member States' lobbying efforts in

---

304 Recital 17(a) during the drafting process.
305 Article 8(3) during the drafting process.
306 'Outcome of Proceedings 9388/92', 19-20; 'Outcome of Proceedings of Working Party on Economic Questions (Data Protection), 29 October 1992' 9918/92, 5.
307 'Note, from the Presidency, Subject: Use of personal-data files in medical research (Personal-record research)' 6454/93.
308 'Note from the German Delegation, 7 June 1993, to General Secretariat for the Council' 7132/93, 6.
309 'Outcome of Proceedings 9918/92', 5.

determining what categories of processing would be used as 'examples' of the public interest as eventually reflected in Recital 34. They recognised the need to substantiate the concept further,[310] but no attempts were made (or at least documented in the *travaux*) to develop a set of objective criteria that would enable Member States and data controllers to determine what types of processing may be in the public interest, or indeed an 'important' public interest for the purposes of the Directive, beside those explicitly indicated examples. Member States continually expressed their concerns that, absent clearer explication of the public interest justifications to processing, certain (and important) forms of processing would be hindered by the Directive given the perceived inability to meet other conditions for processing, such as obtaining consent.

The importance attributed to developing a clearer, substantive understanding of the concept is reflected in these lobbying efforts. Member States attempted to shape the scope of the public interest provisions to meet their own requirements for the concept in context of their own country's data processing needs but also clearly their own contextual understanding of the public interest. This is crucial to the unpacking of the relationship between examples of the public interest given in the Directive and the concept itself – this relationship is devoid of any logic or reasoning aside from the fact that a certain Member State (or States) lobbied for that particular type of processing, either for complete exclusion or partial exemption. No efforts were made to otherwise develop an understanding of what the public interest meant in a fuller and substantive sense although it was clear that the public interest provisions were to play a crucial role

[310] Towards the end of the drafting process in 1994 the Presidency (then Greece) suggested the inclusion of examples of important public interests to interpret Article 8 as to special categories of personal data and as regards to data transfers also made on the basis of important public interests: '(1) To allay concerns expressed by a number of delegations, it is proposed to bring in a general recital on "important grounds of public interest" listing the interests covered by Article 8(3) and the 4th indent of Article 27(1)'. Their suggestion for a recital is similar to the now current Recital 34 in the finalised DPD: 17(a) 'Whereas Member States must be allowed to derogate from some of the provisions of this Directive when justified on important grounds of public interest; whereas, however, they must provide suitable specific safeguards in order to protect fundamental freedoms and privacy; whereas, for example, the following activities must be deemed to constitute matters of important public interest: public health and social protection, scientific research, international exchange of data between tax or customs authorities or between police departments or departments with responsibility for national security'. 'Note: from Presidency date: 14 April 1994 for: Working Party on Economic Questions (Data Protection) 6316/94, 3-4.

in justifying many forms of processing without consent, (e.g. for research, particularly health research, national security, public health etc.).

In reviewing the *travaux* in full, it appears that several countries lobbied for specific types of processing to be excluded or exempt from full application of the Directive. Member States considered such processing critically important and as such that they should not be impeded by the implementation of the Directive. These lobbying efforts focused, in the main, on certain *purposes* for processing special categories of personal data but also at times focused on particular *data controllers*:

- International human rights organisations;[311]
- The medical profession;[312]
- Employment and social security purposes;[313]
- Research and statistics (especially medical research);[314]
- Public safety and state security;[315]
- Religious purposes;[316]
- Political canvassing;[317] and
- Tax collection for funding of churches.[318]

---

311 It is unclear from the *travaux* which Member State lobbied for its inclusion in the Commission's 1992 Compromise Draft. 1992 Compromise Draft, 18.
312 It is also unclear what Member State lobbied for its inclusion, but medical research is consistently raised in regards to research activities more generally. ibid, Recitals 16-17.
313 Lobbied for by Germany. 'Note from the German Delegation, 7 June 1993, to General Secretariat for the Council' 7132/93, 7-8.
314 Lobbied for extensively throughout the legislative process. Considered, for example, in: 'Note, from the Presidency, Subject: Use of personal-data files in medical research (Personal-record research)' 6454/93; 'Addendum to Cover Note, from Belgian Delegation, 30 June 1993, to Mr Niels Ersbøll Secretary-General of the Council of the European Communities' 7695/93; 'Transmission Note, from the Irish Delegation, 8 July 1993, to Working Party on Economic Questions (data protection)' 7859/93, 3; 'Transmission Note, from the Danish delegation, to Working Party on Economic Questions (data protection), 28 July 1993' 8217/93; 'Cover Note, from Presidency, to Permanent Representatives Committee, Subject: Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data - Progress report, 31 August 1993' 8381/93, 3.
315 Lobbied for by France. 'Outcome of Proceedings of Working Party on Economic Questions (Data Protection) on 28, 29 and 30 March 1994' 6153/94, 5.
316 Lobbied for by Germany. 'Outcome of Proceedings of Working Party on Economic Questions (Data Protection) on 28, 29 and 30 March 1994' 6153/94, 5.
317 Lobbied for by the UK. 'Note from Presidency to Internal Market Council' 11581/94, 5; Council of the European Union, 'Report, from Permanent Representatives Committee, on 10 January 1995, to Council meeting (General Affairs), on 6 and 7 February 1995' 4649/95, 2.
318 Lobbied for by Germany. 'Note, from Presidency, 14 April 1994, for Working Party on Economic Questions (Data Protection) 6316/94, 4.

By far the most lobbied for type of processing (insofar as the *travaux* reveal) was for research (especially medical research), for which discussions spanned over two years of the legislative history to the Directive.[319] This merits a closer examination.

2.6.1 The impact of the Directive on research and statistics

The lobbying efforts made by Member States to secure certain derogations for research and statistics can be divided roughly into two camps: 1) those that wanted specific derogations to be added to the relevant Articles with further guarantees in the Recitals; and 2) those that wanted research processing to be addressed in a separate and distinct article within the Directive. It should be noted that not all Member States submitted written evidence as to their positions on this issue and at times various Member States will have changed their position and accepted compromises. Below I consider, chronologically, the various suggestions made and positions taken in regards to how research and statistics would be treated under the Directive. This is important to understand as the resulting compromises that were made involved the introduction of the public interest conditions and public interest examples in Recital 34 of the Directive.

2.6.1.A Autumn 1992 – the public interest provisions as a 'compromise' solution for concerns over research

After the release of the Commission's 1992 Compromise Draft, the Working Party on Economic Questions (Data Protection) continued discussions with delegations on the proposed Directive. As time progressed, and more compromise positions were agreed by Member State delegations, we see that research and statistics continued to be an outstanding issue which remained unresolved until the end of drafting. In October 1992, soon after the 1992 Compromise Draft was released, delegations (including Denmark, France, the Netherlands and the UK) had already expressed their concerns over the potential chilling effect of the Directive on research if written consent was required to process special categories of personal data, notably health data.[320] In reaction, the Commission provided: 'while feeling that these concerns could be covered

[319] By the UK, Ireland, Greece, Denmark, Belgium, Spain, the Netherlands, and Italy.
[320] 'Outcome of Proceedings, of Working Party on Economic Questions (Data Protection), 29 October 1992' 9918/92, 3. ('Outcome of Proceedings 29 October 1992'.)

by the text of Article 7(d) and 8(2)(c)(health), and Article 8(3) (grounds of important public interest), was open to suggestions from the delegations.'[321] This is the first time that we see the public interest justifications for processing (special categories of personal data) considered as potential 'solutions' or compromises for concerns over research and other types of processing involving special categories of data.

As to the public interest provision in Article 8(3) whereby 'Member States may, [on grounds of important public interest] lay down exemptions from paragraph 1 [by national legislative provision or by decision of the supervisory authority]'[322] Greece was the first of many Member States to raise concerns over the lack of clarity of the public interest concept (and indeed what may be considered an 'important' public interest).[323] As noted above, the Commission provided a rather disappointing response to this concern and indicated that while remaining open to future suggestions on how to clarify an 'important public interest' it 'felt it difficult to clarify this notion further.'[324]

2.6.1.B Mid-1993 – inconsistent treatment of the public interest provisions and introduction of a standalone research provision

We see more focused discussions and considerations of the impact of the proposed Directive on research throughout 1993. In May 1993, the Presidency (then Denmark), submitted a 'note' for discussion asking delegations to specifically consider the impact of the Directive (and especially requirements for consent) on the undertaking of medical research as well as on processing for public health purposes and what (if any) exemptions are required.[325] While this note considered the potential regulatory impact upon *medical* research, because the focus was drawn to 'personal-record research', or research conducted on the basis of records rather than direct contact with individuals, this meant that the implications of such discussions were broader and indeed implicated any research conducted on that basis. This demonstrates that research was

---

[321] ibid.
[322] Outcome of Proceedings 29 October 1992, 3.
[323] In a footnote, Greece is noted as requesting that the phrase 'on grounds of important public interest' be clarified. ibid 5 footnote 15.
[324] ibid.
[325] 'Note, from the Presidency, Subject: Use of personal-data files in medical research (Personal-record research), 14 May 1993' 6454/93, 3.

considered from a much broader perspective than from the narrow viewpoint of e.g. clinical research, involving physical interventions with individuals. The focus on records-based research has continued relevance to this day, given the prevalence of reuses of personal data for many forms of research across all disciplines.

A standalone research provision – Article 9(a)

In July 1993, the new Belgian Presidency suggested the introduction of a separate article, Article 9(a), to deal in full with the relevant derogations for research and statistics. However, they also attempted to remove the public interest justification for processing *ordinary* personal data (in Article 7(e)). Briefly, Belgium suggested that the term 'public interest' be removed and changed to 'official authority':

> Article 7
> Member States shall provide that personal data may be processed only if;
>
> (e) processing is necessary for the performance of a task carried out in the exercise of *official authority* vested in the controller or in a third party to whom the data are disclosed;[326]

They explained this change as an 'amendment designed to simplify the text by employing the concept which is more familiar in Community law ("the exercise of official authority") and is used in Article 55 of the EEC Treaty.'[327] This indicated that 'the public interest' was interpreted by Belgium to be merely synonymous with 'processing carried out by public authorities and that carried out by persons or private bodies when exercising official authority.'[328] Moreover, it represents a more restrictive interpretation of the public interest than most likely intended, given earlier indications by the Commission that the public interest was to encompass, for example, research processing where consent could not be obtained. This is an example of inconsistent understanding of the public interest concept – the Commission interpreted the concept in context of the *purpose* of processing to be undertaken (e.g. for research, for public health etc.) as opposed to Belgium's understanding of the concept in context of *who*

---

[326] 'Addendum to Note, from Belgian Delegation, 30 June 1993, to Mr Niels Ersbøll Secretary-General of the Council of the European Communities' 7695/93 ADD 1, 2 (emphasis added) ('Addendum from Belgian Delegation 30 June 1993').
[327] Addendum from Belgian Delegation 30 June 1993, 2 footnote 3.
[328] ibid.

was eligible to undertake processing under the public interest 'banner'.[329] Curiously, although Belgium seemed concerned with the use of the term in Article 7(e) they did not object to its use in Article 8(3) or, arguably, a synonymous term in their proposed Article 9(a) when requiring research to be of 'general interest'.

Returning to the focus on research, as stated above, Belgium introduced a standalone provision for research and statistics which provided that such processing could be carried out without consent if certain conditions were met including:

- The research was 'in pursuit of an aim of general interest';
- The use of personal data was 'necessary';
- Subsequent publication of research findings did not allow identification of individuals, unless approved by a supervisory authority;
- Data be pseudonymised prior to allowing researcher access (direct identifiers swapped with identification numbers, which are then held separately from data to be used by researchers);
- Prior to processing data for research, they must notify the supervisory authority as to data retention periods etc.[330]

This article reveals that the Belgian Presidency considered research too important to be dealt with tangentially in other provisions under the Directive, such as in the public interest justifications in Articles 7(e) and 8(3). In Article 9(a), the justification for processing is conditioned upon research being of an aim of 'general interest' which arguably is synonymous with the 'public interest'. Thus, although Belgium argued to remove the public interest justification for processing ordinary personal data, this did not mean Belgium did not believe in the public interest of research processing. Rather, Belgium's position seemed to be that it is less likely for research to be impeded by the Directive if it is recognised explicitly in a standalone provision.

Moreover, in conditioning the applicability of Article 9(a) upon a finding of 'general interest' in research, Belgium was implicitly making the public interest a key criterion for evaluating the justification of research without consent. They did so without suggesting any criteria that could be used to assess whether research was of 'general

[329] 'Outcome of Proceedings 29 October 1992', 3.
[330] 'Addendum from Belgian Delegation 30 June 1993', 5.

interest'. Thus, while all the derogations applying to research would be clearly contained within the standalone Article 9(a), Belgium did nothing to alleviate the uncertainty surrounding the application of the public interest concept to research or indeed to any other processing contexts. Under Article 9(a) research would remain subject to the uncertain and ambiguous scope of 'general interest', a term synonymous with the Commission's equally unclear suggested public interest justifications for processing.

Support for a standalone research provision

Subsequently, both the Irish and Danish delegations submitted notes in support of Belgium's suggested research and statistic's provision (Article 9(a)).[331] Ireland found a lack of distinction between the level of protection needed when personal data were processed for commercial and administrative purposes versus for research and statistics.[332] In Denmark's note, there is again a change in public interest terminology, from Belgium's 'general interest' to Denmark's suggestion that the application of Article 9(a) be conditioned on the basis that research is of 'paramount importance to society at large'.[333] This is another example of the inconsistent treatment of the public interest concept, where the term is changed to one that is synonymous but equally vague and is left similarly undefined by the suggesting delegation. These discussions were considered far from resolved by the end of August 1993, when the Belgian Presidency flagged that the impact of the Directive on research, and the provisions of Article 8, required detailed discussions in a second reading of the draft Directive.[334]

Discussions continued, with particularly strong lobbying on the use of health data and processing for medical research. Delegations wanted to ensure that Article 8 would be reworded to achieve 'the conditional authorization of the processing of medical data

---

331 'Transmission Note, from the Irish Delegation, 8 July 1993, to Working Party on Economic Questions (data protection)' 7859/93, 3; 'Transmission Note, from the Danish delegation, to Working Party on Economic Questions (data protection), 28 July 1993' 8217/93, 2.
332 ibid 3.
333 Transmission Note, from the Danish delegation, to Working Party on Economic Questions (data protection), 28 July 1993' 8217/93, 2.
334 'Cover Note, from Presidency, to Permanent Representatives Committee, Subject: Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data - Progress report, 31 August 1993' 8381/93, 3.

and not the prohibition of their processing subject to derogation.'[335] For example, France lobbied for much broader derogations for health data and medical research which would include the conditional permission to use health data for research (and other public health reasons) without consent, so long as data subjects do not object to processing. [336] They further suggested that, notwithstanding this conditional authorization and for reasons of 'major public interest', data controllers could also use health data without consent. Here we see the treatment of health data and medical research as 'exceptional'[337] and thus requiring 'special' treatment. The French did not believe it appropriate to regulate health data in the same way as other special categories of personal data, for example data on race and religion which are *justifiably* processed in far rarer circumstances. [338] As to the public interest, yet again inconsistent terminology is used. 'Major public interest' was used by France without definition and is as equally vague as previous iterations of the concept ('important public interest' versus 'major public interest' versus 'general interest' versus 'of paramount importance to society').

The UK Department of Health also submitted a note to address the impact of the Directive on medical research.[339] Their description of the potential, detrimental impact upon public health, improvement of health services and essential research, are a further example of delegations treating health data and medical research as exceptional and requiring 'special' treatment.[340] They lobbied for the separate treatment of research in

---

335 'Outcome of Proceedings, of Working Party on Economic Questions (Data Protection), 1-2 Dec 1993' 11254/93, 4.
336 'Note, from French Delegation, to Working Party on Economic Questions (Data Protection) 17 November 1993' 10242/93, 2.
337 In both the DPD and DPA 1998 health data are treated as special or 'sensitive' categories of data requiring further safeguards to process. Furthermore, in both legislations, processing data for medical research and related purposes are explicitly recognised. DPD, Recitals 33-34 and Art 8(1)-(3); DPA 1998, s 2(e) and Sch 3, para 8. See discussion on the 'exceptional' treatment of health data in the US context: Nicolas Terry, 'Big Data Proxies and Health Privacy Exceptionalism' (2014) 24 65, 87–97.
338 The French delegation stated: 'In the view of the French delegation it is not possible to treat in the same way: – on the one hand the processing of data on race, religion and ... infringing the fundamental rights of individuals and respect for their privacy, such processing being possibly justified only in very rare cases; – on the other hand the processing of data concerning health, which must clearly be flanked by appropriate guarantees but which is normally implemented in the interest of the data subject or of the community and is currently widespread in the EEC.' 'Note, from French Delegation, to Working Party on Economic Questions (Data Protection) 17 November 1993' 10242/93, 2.
339 'Fax, from Andrew P Holt, UK Permanent Representation to the European Communities by the UK Department of Health, to Enrique Gonzalez Sanchez, Council Secretariat, 1 December 1993', 2.
340 ibid.

a standalone provision such as the draft Article 9(a) introduced by the Belgian Presidency.[341] As research and the use of data for various health purposes are included as explicit examples of 'important public interests' in the final DPD, it is important to understand the significant lobbying efforts made by various Member States for these types of processing. This also reminds us that the concept of the public interest remained undeveloped and undefined in a substantive sense – no criteria were suggested to assess the public interest in processing aside from the examples introduced by various delegations. At this stage in the draft Directive, the public interest merely reflected the lobbying efforts being described here. Indeed, after the issues raised by the French and UK delegations, Member States remained unclear precisely what the public interest meant beyond the processing explicitly included in Article 8 such as for public health grounds.[342] As a final note, it is worthwhile acknowledging that despite these lobbying efforts and the explicit mention of research in Recital 34 of the final DPD, research (at least in the UK) continues to be hindered by the culture of caution and legal ambiguity surrounding the use and sharing of data for research.

2.6.1.C January 1994-December 1994 – final lobbying efforts for research

The lobbying efforts for research, made during the last year of negotiations on the Directive, involved some Member States focusing on derogations to be included in various articles, whereas other Member States continued to argue for the separate treatment of research in a standalone provision. For the latter delegations, the public interest provisions (in particular Article 8 on the legal grounds for processing special categories of personal data) were considered insufficient to secure the continued processing of data for research (especially medical research). As an example of the first camp of delegations, Ireland and Portugal lobbied for derogations to be written into Article 14 (dealing with restrictions on data subject rights) that would exempt research processing from subject access requests, for example.[343]

---

[341] ibid.
[342] 'Outcome of Proceedings, of Working Party on Economic Questions (Data Protection), 1-2 Dec 1993' 11254/93, 5.
[343] 'Outcome of Proceedings, of Working Party on Economic Questions (Data Protection, on 20 and 21 January 1994' 4382/94, 6.

As to the second camp of Member States, and in line with their previous arguments for a standalone research provision, the UK delegation submitted a cost-analysis which detailed the potential impact of the Directive on the UK's health service and the undertaking of medical research.[344] In a similar vein, the Spanish delegation also lobbied for the separate treatment of research given its inherent public interest which could only be secured by a standalone research provision:

> In view of the importance of scientific research and statistical studies which are valuable in themselves and as vital factors in social progress, and on the understanding that the Directive must never be used as a means of raising barriers or limiting exchanges of scientific information and is to have a considerable influence on such investigation and studies, they must be given special and independent treatment within the Directive. The proposal made by the Belgian Presidency within the Working Party on Economic Questions (7695/93 ADD 3 ECO 173 of 19 October 1993) which deals both with the processing of special categories of data (Article 8) and with the question of scientific and statistical research (Article 9), could be used as a working basis.[345]

The public interest as a compromise for research

In a critical development of the public interest provisions and the position that would ultimately be taken on research processing, the Greek Presidency suggested a reformulation of Article 8(3) that would explicitly list research and certain health purposes as examples of 'public interest' processing.

> Member States may, on important public interest grounds, grant derogations from paragraph 1, *particularly in* the areas of public health, public statistics or scientific research.[346]

After this suggested reformulation, crucially, Greece suggested it would be the responsibility of Member States, (specifically their data protection supervisory authorities) to develop appropriate guidelines on how to determine when processing is an important public interest:

---

[344] 'Note, from the United Kingdom delegation, analysis of costs, prepared by the Economic and Operational Research Division of the Department of Health, 4 February 1994' 4495/94, 7-8.
[345] 'Note, from the Spanish delegation, to the Working Party on Health Questions, 15 February 1994' 4859/94, 3.
[346] 'Note, from the Presidency, to the attention of the Working Party on Economic Questions (Data Protection), 14 March 1994' 5575/94, 3 (emphasis added).

> The derogations referred to in the preceding subparagraph shall be granted by national legislative provision or by decision of the supervisory authority, stating the types of data which may be processed, the persons to whom such data may be disclosed and the persons who may be controllers, and specifying suitable safeguards.[347]

This is critical because what the Greek Presidency did, and what the other delegations previously had not done, was to add substance (in the form of examples) and potential procedure for assessing the public interest concept. However, these examples seemed to be added only based on what had been lobbied for by other delegations. The use of the phrase 'particularly in', within Greece's reformulation of Article 8(3), indicates that the intention was to introduce a *non-exhaustive* list of examples of what could be characterised as an important public interest. Although we finally see further substance added to the concept of the public interest in the form of these examples, Greece ultimately failed to offer the clarity needed, which would have required the inclusion of relevant criteria that could be used to determine what may be considered an important public interest if it is not explicitly mentioned as such in the Directive.

Remaining conflicts over the public interest compromise

In later considering Greece's proposals, eight Member States[348] were unsatisfied with the proposed Article 8(3) and the addition of examples to secure the processing of data for research and health purposes.[349] These Member States did not believe the reformulation of Article 8(3) was enough to guarantee the unimpeded processing of special categories of data for research and maintained their desire to have research covered by a standalone provision, such as in the Belgian Presidency's suggested Article 9(a).[350] Their dissatisfaction was not further explained, but it is possible that these delegations remained uncertain over the scope of the public interest justifications given that the concept remained insufficiently defined aside from the three examples given. Specific concerns were indeed raised as to the uncertain scope for the suggested public

---

[347] ibid.
[348] Including Denmark, Belgium, Spain, Ireland, the Netherlands and the UK. France and Italy noted being amenable to a standalone research provision. Only Germany supported the Greek Presidency's reformulation of Article 8(3). 'Outcome of Proceedings, of Working Party on Economic Questions (Data Protection), on 28, 29 and 30 March 1994' 6153/94, 4.
[349] ibid.
[350] ibid.

interest justification in Article 8(3). France asked that public safety and state security be named as examples of the public interest, whereas Germany wanted specific reference to processing for religious reasons/by religious communities.[351]

This shows the utter lack of objective criteria being used to develop the public interest concept in the Directive. These suggested examples merely represent the interests of a particular delegation; however, they may suggest an important quality of the public interest – that it is inherently *contextual* and therefore difficult if not impossible to define in an exhaustive sense. Finally, we see another suggested change in public interest terminology proposed by the Netherlands; this delegation wanted the public interest changed to the 'general interest' (similar to Belgium) but again no definition was provided, meaning, one vague term would merely be switched for another.

In regards to the concerns raised by the eight delegations, the Greek Presidency offered a further reformulation of the public interest provision in Article 8(3) and critically a new explanatory recital.[352] First, Greece redrafted Article 8(3) to state:

> 3. Member States may grant derogations from paragraph 1 on important grounds of public interest.
>
> The derogations referred to in the preceding subparagraph shall be granted by national legislative provision or by decision of the supervisory authority setting suitable safeguards.

Thus, they removed the public interest examples encompassed in their initial reformulation of Article 8(3). Rather than develop criteria for determining whether processing is an 'important public interest' they instead added back the examples in a standalone recital:

> To allay concerns expressed by a number of delegations, it is proposed to bring in a general recital on 'important grounds of public interest' listing the interests covered by Article 8(3) and the 4th indent of Article 27(1):

---

[351] ibid 5.
[352] 'Note, from Presidency, 14 April 1994, for Working Party on Economic Questions (Data Protection)' 6316/94, 3.

> 17(a) 'Whereas Member States must be allowed to derogate from some of the provisions of this Directive when justified on important grounds of public interest; whereas, however, they must provide suitable specific safeguards in order to protect fundamental freedoms and privacy; whereas, for example, the following activities must be deemed to constitute matters of important public interest: public health and social protection, scientific research, international exchange of data between tax or customs authorities or between police departments or departments with responsibility for national security'.[353]

In this reformulation, the Greek Presidency acknowledged that Member States were not satisfied with the uncertainty surrounding the public interest concept, if the public interest provisions were to be the sole way of justifying certain 'important' forms of processing without consent. However, rather than developing criteria and a fuller substantive understanding of the public interest, the Greek Presidency merely included the processing types lobbied for by various delegations. This is an important passage in the *travaux* as it does demonstrate a desire to better understand and explicate the public interest concept however it only half-heartedly does so.

Despite this disappointing attempt to clarify the public interest concept, we see that the public interest justifications for processing were intended to be more broadly interpreted than currently understood in practice. This is because the examples of public interests provided for in Recital 17(a) (and that eventually are included in Recital 34 of the final DPD) are prefaced by the words 'for example' indicating a *non-exhaustive* list of public interests. However, without any objective criteria it would (and does) remain a difficult task to determine with any certainty what processing could be covered by this provision if not explicitly listed as an example.

As a final demonstration of the arbitrary way in which the public interest justifications for processing developed, Germany once again lobbied for a public interest to be included within the scope of Article 8(3). The delegation asked that it be recorded that they would treat the processing of data for tax collection to fund religious organisations as an important public interest, *regardless* of whether it would be included in the new Recital 17(a).[354]

---

[353] ibid.
[354] 'Working Document, from General Secretariat of the Council, 17 May 1994, to Delegations' 6285/1/94, 26.

At this stage in negotiations, it was clear that there was a divide between those States that wanted research treated in a standalone provision and those that were satisfied to have research come within the scope of the public interest grounds for processing, as suggested by the Greek Presidency. By May 1994, the Greek Presidency made it clear that they found a standalone research provision, such as Belgian's suggested Article 9(a), unnecessary:

> The Presidency has likewise opposed the introduction of over-detailed provisions aimed solely at clarifying the principles already enshrined in the draft Directive (see in particular the discussions of the Working Party on Scientific Research, Epidemiology and Statistics).[355]

In this document, Greece indicated their belief that the public interest provisions, such as under Article 8(3), were enough to secure the processing of special categories of data for research. At this point eight delegations are recorded as generally in support of the public interest provision,[356] whereas four delegations (Denmark, Germany, Ireland and the UK) found the provision too limiting and wanted Member States to be able to derogate from the prohibition on processing special categories of personal data for *any* reason – not just those in the public interest.[357] Their reasons for objecting to the public interest provision in Article 8(3) is not further explained, but it is reasonable to presume that these delegations found the provision unacceptably vague and thus unreliable for the purposes of securing important forms of processing, such as for medical research, social security purposes etc. Nevertheless, the Presidency suggested retaining Article 8(3) given its support by most delegations. As a 'compromise' the Greek Presidency again suggested that examples of the public interest be given to clarify the concept:

> In order to allay the concerns of various delegations, it may be useful, however, to provide several examples in order to clarify the idea of important public interest. These examples could be provided in either a recital or the actual text of the Article if it is thought that greater legal security is required. They should

---

[355] It seems this Working Party was established as part of the legislative process but was not mentioned elsewhere in the *travaux*. 'Note, from Presidency, 10 May 1994, to Permanent Representatives Committee' 6856/94, 4.
[356] Including, Belgium, Greece, Spain, Italy, the Netherlands, France, Portugal, Sweden.
[357] 'Note, from Presidency, 10 May 1994, to Permanent Representatives Committee' 6856/94, 11.

> include scientific research, in particular epidemiological research, and public statistics.[358]

Again, these specific examples were provided simply because these were the types of processing lobbied for; no effort was given to better define the public interest or provide criteria which could be used to assess the public interest in processing if not explicitly listed as such. This characterisation of the public interest provisions as a compromise for research (among other processing types lobbied for) is made abundantly clear in the Presidency's next statement:

> The Presidency reminds the Committee that the Health Council has pointed to the need to avoid endangering epidemiological research through excessively cumbersome constraints which might arise from this draft Directive. In the view of the Presidency the major concerns voiced in connection with important public interest could be fully satisfied by each Member State. This solution, proposed by the Commission, is supported by a number of delegations (in particular D/F and GR).[359]

This passage is crucially important to understand the intended scope and role of the public interest concept in the DPD. First, it is clear from this statement that the public interest was intended to play a role in justifying several 'important' forms of processing, where consent was not possible (i.e. for research purposes). Second, the lack of clarity on the public interest concept was acknowledged and defining it was a task specifically assigned to Member States whether through guidance and/or legislation ('In the view of the Presidency the major concerns voiced in connection with important public interest could be fully satisfied by each Member State.'[360]) This at least partially explains the current gap in knowledge on the public interest provisions and concept in data protection, as no Member State (to my knowledge) has defined the public interest concept, beyond the descriptive examples provided in the DPD or as a matter of procedure (e.g. in the UK that processing can be justified on the public interest if 'necessary' and related to a function of a 'public nature'). Third and finally, delegating the further refinement of the public interest provisions to the Member States represented an implicit recognition that the public interest concept is inherently context sensitive and impossible to define exhaustively. The context sensitivity of the

---

[358] ibid 12.
[359] 'Note, from Presidency, 10 May 1994, to Permanent Representatives Committee' 6856/94, 12.
[360] ibid.

public interest is something which plays an integral role in my development of the concept and is a factor I pay close attention to in Chapter 4 where I examine the normative dimension of the public interest within theory.

In spite of the apparent compromise, Greece noted a remaining six delegations (Belgium, Denmark, Spain, Italy, the Netherlands and the UK) did not think the public interest provision was enough, on its own, to secure processing for research; these six countries still advocated a standalone research provision.[361] These delegations asserted that only a standalone provision would be able '…to preserve the balance between the protection of the rights of individuals and research and statistical requirements.'[362] The Greek Presidency made their opposition to Belgium's suggested Article 9(a) clear and dismissed it on the basis that: '…far too precise and detailed provisions … are not essential in view of the objectives of the draft Directive.'[363] This reveals a further divide between Member States: 1) those that ascribed to the duality of objectives of the Directive, to not only protect personal data but to also *facilitate* its use versus 2) countries, such as Greece, that clearly found the *facilitation* of data processing, even for 'important' purposes, as secondary.

And so, negotiations continued in light of this divide, with various delegations continuing to lobby for the separate treatment of research in a standalone provision[364], receiving pushback from other delegations on the basis that research and other important forms of processing were sufficiently provided for, specifically by the public interest justifications for processing and its explanatory Recital 17(a). No further compromises were offered to those delegations who believed the public interest provisions insufficient to secure processing for research. Indeed, the public interest

---

361 ibid.
362 'Note, from Presidency, 10 May 1994, to Permanent Representatives Committee' 6856/94, 12.
363 ibid.
364 For example, by Spain, Belgium and the UK: 'Extract from the Draft Summary Record of the 1611th meeting of the Permanent Representatives Committee (part 1) held in Brussels on Thursday 26 May 1994' 7191/94; 'Report, from Permanent Representatives Committee, on 3 June 1994, to Internal Market Council' 7500/94; 'Note, from the UK Delegation, to the Working Party on Health Questions, 21 September 1994' 9415/94, 5-6; 'Cover Note, from General Secretariat of the Council, to Permanent Representatives Committee/Council, 14 November 1994' 10934/94; 'Extract from the Draft Summary Record of the 1628th meeting of the Permanent Representatives Committee Part 1 held in Brussels on 14 November 1994' 10957/94.

examples provided in Recital 17(a) were considered all that was needed to allay these concerns even though the Recital provided no objective criteria to assess the public interest in processing:

> The present text gives Member States the option of providing for additional derogations to the prohibition for reasons of major public interest. This idea of major public interest is, moreover, made clear in recital 17(a), which gives several examples and refers inter alia to scientific and statistical research. However, the [Belgian] and [Spanish] delegations, supported by UK, could not settle for scientific research and statistics being covered only by this paragraph, and wanted a separate Article for those fields. ([Spain] made particular reference to the need for legal certainty in those two areas).[365]

The lobbying for the separate treatment of research reflected concerns over legal uncertainty if data controllers were forced to rely on the ambiguous public interest provision in Article 8(3). It was clear from the remainder of negotiations on the Directive that further clarification would not come – the public interest provisions and examples of important public interests in Recital 17(a) would need to be sufficient. Insofar as delegations continued to raise their concerns regarding the potential chilling effect of the Directive, and the perceived need to obtain consent for various forms of research:

> Article 7 of the amended proposal provides a clear response to this. The processing of data needed for research or statistical purposes will either require the consent of the data subject, be covered by the 'balance of interest' clause or be necessary for a task in the public interest that is to be performed by the controller.[366]

As most discussions regarding the public interest were focused on Article 8(3) (the legal ground for processing *special categories* of personal data), this is notably one of the few (if not only) documents within the *travaux* that explicitly recognises Article 7(e) and thus the public interest as an alternative route to justifying the use of *ordinary* personal data for research. In this regard, the Presidency (then Germany) offers an example of processing that would be justified based on Article 7(e) in the public interest:

---

[365] 'Report, from Permanent Representatives Committee, on 3 June 1994, to Internal Market Council' 7500/94, 6.
[366] 'Working Document, from Presidency, concerning statistics/scientific research problems, 20 July 1994' 8525/94, 3.

> Processing undertaken for the purpose of compiling statistics in the public interest - an exercise in which data subjects are obliged to take part - within the framework of programmes being implemented by the national statistical offices is obviously regarded as a task in the public interest.[367]

Two things are important to note from this example. First, the example is *not* regarding research *per se* but rather government collection of statistics which may imply a narrower interpretation of the public interest provision in Article 7(e) as applicable to processing by a public authority. Second, even if this was not the intended interpretation of this example, no other guidance is offered as to what other forms of processing might meet the public interest threshold; the Presidency merely provides that such a task is 'obviously' regarded as in the public interest.

The German Presidency attempted to further address concerns of the delegations regarding Article 8(3) by making absolutely clear the purpose of the public interest justification for processing:

> This criterion of important public interest, applied to research and statistics, refers precisely to the areas covered by the Danish delegation in the expression 'scientific and statistical research of major importance to society as a whole'. It is for the Member States to specify both the suitable safeguards and the decision-making procedures for such processing as is provided for in Article 8(3) (authorization by law or by a supervisory authority).[368]

Thus, the public interest provision in Article 8(3) was intended to justify, where necessary, the use of special categories of data for research and statistics as well as other important forms of processing. However, given the lack of criteria to independently assess the public interest in processing, the question remained as to how Member States were to determine precisely whether a type of processing was in the public interest. As applied to research, what could be considered of 'major importance to society as a whole'? Furthermore, given the interplay between Articles 8(3) and 7(e) how does the public interest differ between the two provisions? What *is* the difference between an 'important public interest' and an ordinary 'public interest'? The latter likely implying a lesser standard. The German Presidency provided that Member States were

---

[367] ibid.

[368] 'Working Document, from Presidency, concerning statistics/scientific research problems, 20 July 1994' 8525/94, 3.

responsible for ensuring that the public interest justifications were deployed with appropriate safeguards. In examining the text of the public interest conditions in the DPA 1998, the extent to which this task was fulfilled in the UK can be determined.

2.7 Final position on the public interest provisions

Those that desired further clarification of the public interest provisions were left disappointed in the concluding phases of drafting the Directive. The examples of the public interest provided in Recital 17(a) were considered sufficient to allay these concerns despite the lack of criteria to independently facilitate an assessment of the public interest in processing. It was considered that despite this crucial explanation being a mere recital, that:

> The Council and the Commission note that the elements set out in recital 17(a) of the Directive, which are intended in particular to clarify the concept of public interest in Articles 7 and 8 of the Directive, derive from the purpose of the latter and thus form an integral part of this legal act; it follows that those elements are to be taken into consideration by the Member States when they adopt the laws, regulations and administrative provisions required to comply with the Directive.[369]

First, it must be acknowledged that this statement provides the clearest indication in the *travaux* as to the intent of the legislators on how the public interest should be interpreted. Second, this piece of interpretative information is meagre and fails to deliver the clarification needed on the *substance* of the concept. Although they refer to 'elements', there are no criteria to guide independent assessments of the public interest in processing – there are only examples which are indicative of nothing more than the lobbying efforts of Member States. The only 'elements' to speak of in Recital 17(a) are: 1) that the processing be an 'important public interest' and 2) the public interest justification must be subject to specific and suitable safeguards to protect the fundamental rights and the privacy of individuals. Without any indication of how to determine the public interest in processing, or indeed how 'important' a public interest must be to justify the use of *special* categories of personal data, Member States would fail to implement even the first of these supposed elements.

---

[369] 'Extract from the Draft Summary Record of the 1628th meeting of the Permanent Representatives Committee Part 1 held in Brussels on 14 November 1994' 10957/94, 9.

The quote above was requested to be entered into the Council's *minutes*, presumably, to ensure that Recital 17(a) (finalised as Recital 34) was used to guide the interpretation of the public interest concept. Nonetheless, to my knowledge, this statement which provides essentially the only guidance (however meagre) for interpreting the public interest within this legislation (and Member State legislation) is not widely known, if at all. This would justify Denmark's remaining concerns that important forms of data processing, such as for research[370], should not have been dealt with tangentially in footnotes and recitals to the legislation:

> The Presidency has presented a compromise proposal attempting to take account of the special requirements for the processing of personal data in the areas of research and statistics. The compromise proposal is based on interpretations in the 'Whereas clauses' of the scope of the articles of the directive, and also on an interpretative statement in the Council minutes in relation to research and statistics. Denmark considers it unacceptable that such important decisions on derogations from the general rules should be based on interpretations in the preamble and statements in the minutes - which are normally not made publicly available, - but considers that they should be reflected directly in the Articles of the directive.[371]

In summary, the final position taken on the public interest provisions was essentially to 'pass the buck' to Member States to legislate as appropriate to clarify the substance and necessary procedure for these provisions. The Council and Commission were satisfied that the public interest provisions offered sufficient legal certainty to allow important forms of processing, such as research, to proceed unimpeded. No standalone provision for research was ever adopted. The uncertainties which continue to plague subsequent implementation of the Directive across Member States, noting

---

[370] Denmark was the only delegation to explicitly raise concerns about the impact of the Directive on *social sciences* research: 'Denmark has stressed strongly during the negotiations that the present wording is too restrictive. Basic research today is to a large extent based on the establishing and running of registers (databases), especially within medical research, and the directive as proposed may hinder important sociological, historical and medical research as well as statistical work.' As stated in previous sections, discussions regarding research primarily focused on medical research. But discussions were at times broad enough to encompass other disciplines e.g. when personal record research was referenced. ('Note from the Presidency, 14 May 1993, on 'Use of personal-data files in medical research (Personal-record research) 6454/93, 3.) Furthermore, the use of the term 'scientific research' in Recital 17(a) (and eventually Recital 34) is generic enough to encompass social sciences and humanities research as well. 'Cover Note, from General Secretariat of the Council, to Permanent Representatives Committee/Council, 14 November 1994' 10934/94, 3.

[371] Note from the Presidency, 14 May 1993, 3-4.

the predominance of the consent-or-anonymise paradigm to justify research uses of data, seems to validate the concerns of Denmark and other similarly-minded delegations.[372] Moreover, it signifies the lack of legal certainty surrounding the public interest provisions in the Directive and the resulting lack of confidence that data controllers have to rely on them.

2.8 Concluding thoughts on the DPD's legislative history

The protracted negotiations which comprise the legislative history of the DPD reveal the intended *purpose* of the public interest provisions while its *scope* was left more uncertain. The public interest provisions, from the earliest drafting stages, were intended to operate as justifications for certain 'important' forms of processing where the obtaining of consent was considered a disproportionate barrier. This reveals the integral role of the public interest justifications for processing and thus the imperative for developing a clearer understanding of the public interest concept in data protection which is the aim of my contribution.

To clarify the public interest justifications for processing, examples were provided in Recital 17(a) which explicitly named the specific processing types that Member States lobbied for, including for research and statistical purposes. While the Council and Commission were explicit in their intentions for Member States to take *specific* account of Recital 17(a) (eventually Recital 34) when considering the public interest provisions, there remains legal uncertainty as to the precise meaning of the concept and its intended scope. They left this important instruction in the Council minutes and it has remained buried there to the detriment of affording more legal certainty around the public interest provisions. Regardless of the descriptive examples provided, no criteria were ever suggested as to how Member States could assess the public interest in the processing of data.[373] Therefore what can and cannot be established, with any certainty, as to the public interest concept within the Directive? It is *certain* that:

---

[372] See Chapter 2 Sections 2 and 4.
[373] 'Extract from the Draft Summary Record of the 1628th meeting of the Permanent Representatives Committee Part 1 held in Brussels on 14 November 1994' 10957/94, 9.

- The public interest provisions were intended to play a role in justifying the processing of both ordinary and special categories of personal data where consent or other provisions were not able to be satisfied.
- The examples of 'important' public interests provided in the explanatory recital were intended to guide interpretation of the public interest provisions in *both* Articles 7(e) and 8(4)[374], but the list of examples were non-exhaustive.
- The public interest provisions were applicable only insofar as Member States ensured 'specific and suitable safeguards' were provided 'so as to protect the fundamental rights and the privacy of individuals'.
- Member States were delegated the responsibility of determining and therefore clarifying the permissible scope of the public interest provisions, in terms of what safeguards were required to avail of the provisions (e.g. what type of data controller could justify processing under Article 7(e) and 8(4)).

However, the 'substance' of the public interest concept and how it applies to different processing contexts, remains more uncertain:

- What objective criteria should be used to assess the public interest or 'important' public interest in processing if the type of processing is not within the explicit list of examples in the Directive?
- Indeed, is any processing of data that falls within one of the specifically listed types enough to meet the ambiguous public interest/important public interest threshold of Article 7(e) or Article 8(4)?
- What is the difference between a 'public interest' and 'important public interest' for the purposes of interpreting Article 7(e) as to ordinary personal data versus Article 8(4) as to special categories of personal data? If differing standards apply to Article 7(e) and Article 8(4) how is this assessed?
- What are the specific and suitable safeguards needed to protect individuals' fundamental rights and freedoms, and precisely how are they implicated when decisions to process data are justified based on a public interest served?

The remainder of this chapter examines the DPA 1998 to consider how the UK has implemented the public interest provisions and the extent to which these uncertainties have been resolved.

[374] Discussions until now refer to *Article 8(3)* as to the public interest provision for special categories of personal data. However, Article 8(3) was finalised as Article 8(4) in the DPD.

3. The DPA 1998's Public Interest Conditions

The 'public interest' provisions of Article 7(e) and 8(4) under the finalised DPD were indeed transposed into the UK's DPA 1998. Article 7(e) was transposed into the conditions required for processing ordinary personal data under Schedule 2 paragraph 5(d). Article 8(4) was later transposed into various conditions required for processing 'sensitive' (synonymous with 'special') personal data under Schedule 3, some of which were only added when the DPA 1998 was amended with the DPPSPD 2000.

In consideration of the legislative history of the DPD, Member States were to take specific account of Recital 34 when implementing their own public interest provisions. They were to provide specific and suitable safeguards, protective of individuals' rights and freedoms, where the public interest provisions were used to justify processing. Moreover, further clarification of the public interest concept was a task specifically left to Member States. Did the UK parliament follow these instructions and provide the necessary clarity to the public interest provisions?

3.1 DPA 1998, Schedule 2 paragraph 5(d) – ordinary personal data and the 'public interest'

Schedule 2 paragraph 5(d) provides that the processing of ordinary personal data is lawful to the extent that it is necessary 'for the exercise of any other functions of a public nature exercised in the public interest by any person'.[375] Unlike the equivalent provision in the DPD Article 7(e), this provision provides safeguarding criteria while still not providing any definition of the public interest concept itself. Four separate elements can be extracted from Schedule 2 paragraph 5(d), each of which would need to be satisfied if data processing were justified on this basis. These four elements require that:

1) The processing of personal data is *necessary*;
2) The processing is undertaken as an exercise of a function of a *public nature*;
3) The act is exercised in the *public interest*; and
4) Can be undertaken by *any person*.[376]

[375] DPA 1998, Sch 2, para 5(d).
[376] ibid.

Each of these elements will be considered below to determine how these may relate to the required safeguarding of individuals' rights and freedoms, and more generally, how their interpretation may resolve uncertainty surrounding the public interest concept.

3.1.1 Is the processing of personal data 'necessary'?

This first element of Schedule 2 paragraph 5(d) requires that the use of personal data be 'necessary'. The term is not defined within the DPA 1998 but there is brief discussion in the legislative history on the *purpose* of 'necessary' within the public interest condition.[377] Lord Williams of Mostyn provided:

> The amendment in the name of the noble Viscount, Lord Astor, would add a restriction to paragraph 5(d). We do not believe it is necessary because *paragraph 5(d) already contains safeguards. First, the processing must be necessary*; secondly, the functions must be public functions; and, thirdly, they must be exercised in the public interest.
> …
> We do not see any benefit in the addition of the word 'similar'. The amendment would require those other functions to be similar to those of the Crown and central government. I cannot presently think of any such functions. We feel it adds a restriction which is too restrictive and unnecessary. I hope that I have demonstrated that the safeguards are fully contained within sub-paragraph (d).[378]

Thus, the qualification that the processing of personal data in the public interest must be *necessary* was added as a *safeguard* to individuals' rights and interests where they are not consenting to the use of data.

As to the *meaning* of 'necessary', the term must be interpreted according to the relevant rules of statutory construction. When it comes to interpreting UK law which is an

---

[377] In *Pepper v Hart* [1992] UKHL 3, [1993] 1 All ER 42 [64], Lord Browne-Wilkinson held that 'reference to parliamentary material should be permitted as an aid to the construction of legislation which is ambiguous or obscure or the literal meaning of which leads to an absurdity. Even in such cases references in court to parliamentary material should only be permitted where such material clearly discloses the mischief aimed at or the legislative intention lying behind the ambiguous or obscure words.' The term 'necessary' in the DPA 1998, Sch 2, para 5(d) is sufficiently ambiguous (undefined) to warrant examination of the relevant parliamentary material in Hansard and the material referenced here is clearly regarding this provision. The term's ambiguity is highlighted extensively in Section 3.1.1.

[378] HL Deb 23 February 1998, vol 586, col 28gc (emphasis added).

implementation of EU law, courts are obliged to take a *purposive* approach to interpretation, as opposed to a *literal* approach where the natural and plain meaning of terms are adopted.[379] A literal interpretation of 'necessary' would require that the use of personal data must be 'indispensable, vital, essential; requisite.'[380] However, with a *purposive* approach to interpretation, the purpose and intent behind the use of 'necessary' by the framers of the Directive must be considered.[381]

As under the DPA 1998, the term 'necessary' is not defined in the DPD, and the *travaux* does not reveal detailed discussions regarding its meaning. However, if we examine the context in which the term 'necessary' is situated within the DPD, the broader purpose for its inclusion can be assessed. In the DPD, 'necessary' is used to condition justifications for processing without consent.[382] Data subjects are 'protected' because the use of personal data must not merely be convenient or desirable to the data controller; the use of personal data must be 'necessary' – it must be *required* to serve the relevant public interest.

Similarly, under the DPA 1998, 'necessary' is a condition for the reliance on any other justification for processing without consent. However, subsequent interpretation of the term within the UK, in case law and various guidance materials, reveals divergent understandings of 'necessary'. Case law and other guidance demonstrates uncertainty as to:

> Whether 'necessary' means the processing must be 'essential' or 'indispensable' to meet the processing aims, or a lesser standard of being merely one appropriate route out of several; and whether there is any need for the processing to be proportionate.[383]

---

[379] On the authority of *Bulmer* (n 254) [425]. Per Lord Denning, courts must not '… examine the words in meticulous detail. No longer must they argue about the precise grammatical sense. They must look to the purpose or intent ... They must not confine themselves to the English text. They must consider, if need be, all the authentic texts ... They must divine the spirit of the treaty and gain inspiration from it. If they find a gap, they must fill it as best they can. They must do what the framers of the instrument would have done if they had thought about it'.
[380] 'Necessary' in *Oxford English Dictionary* (3rd edn, 2003).
[381] *Bulmer* (n 254).
[382] DPD, Articles 7(a)-(f); DPA 1998, Sch 2, para 1-6.
[383] Black and Stevens (n 11) 103.

For example, the UK's ICO has wavered on its own interpretation of necessary. The ICO provided in its 2001 guidance that 'necessary' means that the purposes for processing 1) must be valid and 2) can *only* be achieved through the use of personal data.[384] This would on its own imply a *literal* interpretation of necessary in the most restrictive sense, however, a third condition provides that to be 'necessary', processing must be *proportionate* to the aim pursued,[385] thereby reflecting a more purposive approach in line with European jurisprudential principles.[386]

Subsequently, the ICO modified its test for 'necessary'. From 2010 onwards, their guidance provided that necessary should be interpreted as follows:

> This imposes a strict requirement, because the condition will not be met if the organisation can achieve the purpose by some other reasonable means or if the processing is necessary only because the organisation has decided to operate its business in a particular way.[387]

This post-2010 guidance drops the provision that necessary means processing personal data must be the *only* way to achieve the purpose in question (as provided in the 2001 guidance). Thus, this guidance may suggest a lesser standard: that data controllers must substantiate reasons for the use of personal data beyond mere convenience but this does not require strict necessity. This inconsistency was, however, resolved by case law interpreting the meaning of 'necessary' in the UKSC decision in *South Lanarkshire Council v Scottish Information Commissioner*.[388]

This decision, from 2013, focused on the meaning of 'necessary' in Schedule 2 paragraph 6 of the DPA 1998, otherwise known as the 'legitimate interests' condition. 'Necessary' was considered in context of its meaning in European law. Citing *Huber v*

---

[384] This 2001 version of the guidance is now only available via the Internet Archive Wayback Time Machine. ICO, 'Data Protection Act 1998 Legal Guidance' (2001) para 3.1.6 (emphasis added).
[385] ibid.
[386] Specifically, as to the principle of proportionality. See *Gillow v the United Kingdom* (1986) Series A no 109, para 55 as originally developed in *Handyside v the United Kingdom* (1976) Series A no 24, paras 48-49.
[387] This refers to guidance updated on 11 May 2016; however, this change in approach to 'necessary' was made in 2010 – I have kept this version on file but it is also available via the Internet Archive Wayback Time Machine. ICO, 'The Guide to Data Protection' (n 26) 100.
[388] *South Lanarkshire Council v Scottish Information Commissioner* [2013] UKSC 55.

Bundesrepublik Deutschland[389], Lady Hale refers to Member States' obligation to interpret 'necessary' consistently and according to its independent meaning in *European* law:

> …the concept of necessity laid down by Article 7(e) of Directive 95/46… cannot have a meaning which varies between member states. It therefore follows that what is at issue is a concept which has its own independent meaning in Community law and which must be interpreted in a manner which fully reflects the objective of that directive, as laid down in Article 1(1) thereof.[390]

Helpfully, Article 7(e), which was the focus in *Huber*, is the equivalent provision under consideration here i.e. Schedule 2 paragraph 5(d). Lady Hale adopts from the Advocate General's opinion in *Huber* this definition of 'necessary':

> It is well established in community law that, at least in the context of justification rather than derogation, 'necessary' means 'reasonably' rather than absolutely or strictly necessary…[391]necessity is well established in community law as part of the proportionality test. A measure which interferes with a right protected by community law must be the least restrictive for the achievement of a legitimate aim. Indeed, in ordinary language we would understand that a measure would not be necessary if the legitimate aim could be achieved by something less.[392]

On this authority, 'necessary' means that for the purposes of interpreting paragraph 5(d), the processing must be *proportionate* such that the use of personal data is the *least restrictive means* of achieving the public interest aim sought. Although it is important to distinguish proportionality in its purest sense (i.e. ensuring a fair balance between different rights and interests) from its role as part of the test of necessity in EU law, a 'proportionate' approach to 'necessary' aligns with the more recent guidance issued by the ICO (even if the explicit words proportionate are not used).[393] Thus, 'necessary' can be taken to mean that the use of personal data is more than a matter of mere

---

[389] *Huber v Bundesrepublik Deutschland* C-524/06 (2008) ECR I-9705.
[390] ibid, para 52 (emphasis added).
[391] Lady Hale cites: *R v Secretary of State for Employment, ex parte Seymour-Smith (No 2)* [2000] 1 All ER 857, [2000] IRLR 263, [2000] 1 WLR 435; *Chief Constable of West Yorkshire Police v Homer* [2012] UKSC 15, [2012] 3 All ER 1287, [2012] ICR 704.
[392] *South Lanarkshire Council* (n 388) [27], Lady Hales cites the Opinion of Advocate General Poiarest Maduru in *Huber* (n 389) para 52.
[393] Proportionality, as a concept with its own independent meaning must be distinguished from whether the processing of personal data is 1) 'necessary' in the sense of requirement for the achievement of a particular goal and 2) whether the least restrictive means are deployed.

convenience to the data controller, but it need not be essential to the public interest aim sought.

However, there are some caveats to the approach taken to 'necessary' in *South Lanarkshire*. First, Lady Hale cited the Advocate General's definition of 'necessary' which was not ultimately adopted by the ECJ in *Huber*[394] – rather the ECJ merely referred to the fact that the term had its own meaning in Community law and that this meaning must be used by Member States when interpreting the DPD and their implementing legislation, without defining the term themselves.[395] Second, in *South Lanarkshire*, the circumstances of the case were not considered to engage Article 8 of the ECHR, as the identities of data subjects could not be discerned from the data at issue. Thus, it is possible that the balancing of interests and rights required in the 'legitimate interests' condition reflects a lesser standard of 'necessary' than required where an individuals' Article 8 Convention rights are clearly engaged. In sum, a different standard and meaning of 'necessary' could potentially be applied where Article 8 is engaged and overlaps with a case involving reliance on the public interest condition. This is possible given that unlike the legitimate interests condition in paragraph 6, paragraph 5(d) does not explicitly require a balancing of interests between the data controller and data subject.[396] Nevertheless previous authorities agree that 'necessary' must be interpreted according to its meaning in European Law, for example as provided in the opinion by Mr Justice Davis in the English High Court case *Michael Stone v SE Coast Strategic Health Authority*:

> It is common ground that the word 'necessary', as used in the Schedules to the 1998 Act, carries with it the connotations of the European Convention on Human Rights: those include the proposition that a pressing social need is involved and that the measure employed is proportionate to the legitimate aim being pursued.[397]

Again, more recent case law would seem to suggest the 'reasonable' approach to 'necessary', one which incorporates the principle of proportionality, is the meaning

---

[394] Regardless, Lady Hale adopts the predominant definition of 'necessary' from European law and considers it 'uncontroversial' to apply to the case at hand. *South Lanarkshire Council* (n 388) [27].
[395] *Huber* (n 389) para 52.
[396] Lady Hale makes this distinction herself in *South Lanarkshire* (n 388) [25].
[397] *Stone* (n 85) [60].

with the most support in the UK. In 2014, the Upper Tribunal dismissed an appeal against the refusal to disclose photographs of a flat after a fire because disclosure was considered unfair and not 'necessary' for the claimant to prevent future fires in his neighbour's flat.[398] In line with Lady Hale's opinion that 'necessary' be interpreted 'reasonably', Judge Jacob considered that:

> …necessary does not mean that it must be essential or indispensable for him to see the material. That is too strict a test. It is not how the word is used in everyday language. To take a slightly factitious example, 'I need a drink' does not mean that I will die or suffer irreparable kidney damage if I don't have one. Lawyers usually convey this less stringent test by qualifying necessary with reasonably. In truth, this is not a qualification; it merely emphasises how the word is generally used. [399]

Judge Jacob goes on to distinguish between a stricter standard and the reasonable one he adopts:

> Necessary connotes a degree of importance or urgency that is lower than absolute necessity but greater than a mere desire or wish. As a word in everyday use, it does not require, or for that matter allow, further elaboration. It merely has to be applied, which I now do.[400]

Here, Judge Jacob is explaining that to interpret 'necessary' *reasonably* is *not* indicative of a lesser standard; reasonableness merely reflects the approach to 'necessary' in European law. Although Judge Jacob does not directly mention 'proportionality', it is likely that he interpreted 'reasonable' to mean use of personal data that is *proportionate* to the aim sought. Indeed, he cites Lady Hale's definition of 'necessary' in *South Lanarkshire* such that processing will not be considered necessary 'if the legitimate aim could be achieved by something less'.[401]

Even more recently, the UKSC held that certain data sharing provisions within the controversial 'named person scheme' in Scotland[402] were incompatible with Article 8

---

398 *Farrand v Information Commissioner and another* [2014] UKUT 310 (AAC).
399 ibid [26].
400 ibid [27].
401 *South Lanarkshire* (n 388) [27].
402 'What Is a Named Person?' (*Scottish Government*) <http://www.gov.scot/Topics/People/Young-People/gettingitright/named-person>; Stuart Nicolson, 'What Is the Named Person Scheme?' (*BBC News*, 28 July 2016) <http://www.bbc.com/news/uk-scotland-scotland-politics-35752756>.

of the ECHR on the basis of potentially disproportionate interferences with the rights and freedoms of young people and their families.[403] Here, the UKSC again referenced the European approach to interpreting 'necessary' via the proportionality test.[404] They further held that the application of the proportionality test and thus determining the necessity of data processing depends on the *context* of the circumstances. Where Article 8 is engaged, 'necessary' must be deployed in a way that '[recognises] the need to weigh the importance of the disclosure in achieving a legitimate aim against the importance of the interference with the individual's right to respect for her private and family life.'[405]

It was not enough that the relevant provisions in Part 4 of the Children and Young People (Scotland) Act 2014 allowed the disclosure of personal data to a third party if it was considered that data are 'likely to be relevant' to the exercise of certain statutory functions by the third party and 'ought to be provided for that purpose'.[406] The UKSC emphasised:

> Disclosure where the data processor considers that the information is likely to be relevant cannot be regarded as necessary if the legitimate aim could be achieved by something less. It cannot be 'necessary', in that sense, to disclose information merely on the ground that it is objectively relevant, let alone on the ground that a particular body considers that it is likely to be relevant. *Relevance is a relatively low threshold: information may be relevant but of little significance.* A test of potential relevance fails to recognise the need to weigh the importance of the disclosure in achieving a legitimate aim against the importance of the interference with the individual's right to respect for her private and family life. That deficiency is not made good by the requirement that the data controller considers that the information ought to be provided.[407]

It is unclear how the assessment of necessary via the test of proportionality in *The Christian Institute* case differs from the 'reasonable' approach suggested by Judge Jacob in *Farrand* ('Necessary connotes a degree of importance or urgency that is lower than absolute necessity but greater than a mere desire or wish').[408] The UKSC does not seem

---

[403] *The Christian Institute and others (Appellants) v The Lord Advocate (Respondent) (Scotland)* [2016] UKSC 51 [100]-[101].
[404] ibid [56].
[405] ibid.
[406] ibid citing Children and Young People (Scotland) Act 2014, Pt 4, s 26(2)(a)-(b).
[407] ibid (emphasis added).
[408] *Farrand* (n 398) [27].

to advocate a standard of *strict* necessity, but at least where Article 8 is engaged, the use of data must not be merely objectively relevant but be 'significant' to the public interest aim sought.[409] This introduces yet another term without a clear definition. However, the lack of safeguards within the legislation, to protect individuals from disproportionate interferences with their rights under Article 8, appeared to heavily influence the UKSC's reasoning.[410] This suggests that the provision of suitable safeguards is critical to relying upon justifications for using data without consent, regardless of the public interest aim sought. It demonstrates a judicial focus on the safeguards surrounding the application of the public interest to a particular set of facts rather than whether a use of data is *substantively in* the public interest.[411]

The requirement that processing be 'necessary' is clearly a complex topic that has been subject to disagreement over a literal or 'strict' definition of the term. Moreover, recent case law would suggest that in applying the European test of proportionality to the assessment of necessity, that this must be interpreted in context. Therefore the standard that applies may vary depending on the nature of the factual circumstances, including if Article 8 is engaged. Ultimately, to rely on paragraph 5(d), what *is* clear is that data controllers' must establish reasons for needing to process personal data *beyond* mere convenience or desire to do so. What is less clear is the precise threshold to be met if the use of personal data is to be established as 'necessary'.

After *The Christian Institute*, what does it mean for data to be 'significant' to a particular use? 'Necessary' as assessed via the test of proportionality will always require close inspection of the facts in each case, what safeguards are provided, and whether anonymised data could be used instead. In summary, 'necessary' is indeed intended to provide safeguards to data subjects when their consent is not obtained, most recently evidenced by the overturning of the data sharing provisions of the Scottish named

---

409 *The Christian Institute* (n 403) [56].
410 ibid [100]-[101].
411 The UKSC swiftly dealt with the issue of the 'public interest' as being 'obvious': 'As to the first of those questions, it can be accepted, focusing on the legislation itself rather than on individual cases dealt with under the legislation, that Part 4 of the 2014 Act pursues legitimate aims. The public interest in the flourishing of children is obvious. The aim of the Act, which is unquestionably legitimate and benign, is the promotion and safeguarding of the wellbeing of children and young persons.' ibid [91].

person scheme.[412] In assessing whether processing is 'necessary', one can disqualify uses of data that are unable to meet the safeguarding requirements of the public interest conditions. Similar to issues in defining the 'public interest' in a substantive sense, it is also difficult to define 'necessary' any more precisely. Thus, it offers little in the sense of clarifying the substantive meaning of the 'public interest'.

3.1.2 Is the processing a function of a 'public nature'?

The second element to satisfying the public interest condition for ordinary personal data is that processing must be 'undertaken as an exercise of a function, of a public nature.'[413] What is essential to this requirement is that the processing be a function of a *public nature*, which is yet another undefined term within paragraph 5(d), although it has been considered in analogous areas of law, discussed below. First, however, there is brief discussion relevant to the meaning of 'public nature' by Parliament when drafting the DPA 1998.[414] In discussing the purpose of paragraph 5(d), Lord Williams of Mostyn provided:

> Schedule 2 follows Article 7 of the directive very closely. That article sets out conditions which must be met if processing is to meet the fair and lawful requirement in the first data protection principle. Paragraph 5 deals with processing which is necessary in the public interest. *The first three paragraphs are intended to cover processing such as that carried out by the courts, by central government and by those exercising statutory functions. There may be other circumstances where the public interest requires data to be processed. That is the purpose of paragraph 5(d).*[415]

Importantly, Lord Mostyn is distinguishing between processing carried out by public authorities such as courts, government departments and others carrying out statutory functions on the one hand, and processing carried out in the public interest on the other. Therefore, processing of a 'public nature' is not confined to processing which is carried out by a particular public authority or under a statutory mandate. However, it remains unclear precisely *who* (the type of data controller) may satisfy the 'public nature' requirement, and *what* type of processing this encompasses.

---

[412] ibid [106].
[413] DPA 1998, Sch 2, para 5(d).
[414] The term 'public nature' in the DPA 1998, Sch 2, para 5(d) is sufficiently ambiguous (undefined) to warrant examination of the relevant parliamentary material in Hansard and the material referenced here is clearly regarding this provision (see *Pepper* note 377 on consideration of parliamentary material).
[415] HL Deb 23 February 1998, vol 586, col 28gc (emphasis added).

As to answering the question of *who* may carry out processing of a 'public nature', the literature suggests that the use of the term 'public' does not preclude use by a non-public entity, especially in light of the fact that 'any person' can satisfy the condition per the fourth element of paragraph 5(d).[416] The Ministry of Justice supports this interpretation in its 2012 data-sharing guidance, which provides that the public interest condition encompasses:

> processing by voluntary organisations or private bodies, provided that it is in support of a public function that is in the public interest – for example, the reservation of beds in hostels run by a voluntary body for persons registered with local authorities as homeless.[417]

This means that to establish the public nature of processing, it is less about *who* undertakes the processing and more that it relates to a *public function* in the *public interest*. The guidance does not indicate the extent to which the function must be one that is typically 'public' or, in other words, typically undertaken by a public authority, even if outsourced to a commercial organisation. Indeed, what are categorically 'typical' public functions for the purposes of paragraph 5(d)?

Given that 1) 'public nature' and 'public functions' are left undefined and 2) there is a lack of case law on this issue, it is useful to consider how this terminology is interpreted in analogous areas of law. Under the Human Rights Act 1998 ('HRA 1998'), which extends the application of the ECHR to the actions of public authorities in England and Wales, similar terms are used.[418] In section 6, public authorities are defined as:

> (a) a court or tribunal, and

---

[416] Rosemary Jay suggests that 'It is possible, however, for some private or quasi-private bodies to exercise public functions and therefore rely on this condition'. Indeed, this is increasingly the case with the prevalence in outsourcing public functions to private sector organisations. Jay (n 27) 215. This interpretation finds further support in Scotland where the Scottish Government has provided that Sch 2, para 5(d) would support processing undertaken by 'voluntary organisations or private bodies provided that it is in the public interest'. Scottish Executive, 'Data Sharing: Legal Guidance for the Scottish Public Sector' (2004) 30 <http://www.scotland.gov.uk/Publications/2004/10/20158/45768>.

[417] Ministry of Justice, 'The Data Sharing Protocol: Annex H, Legal Guidance on Data Sharing' (2012) 16 <http://webarchive.nationalarchives.gov.uk/20150730125042/http:/www.justice.gov.uk/information-access-rights/data-protection/data-sharing>.

[418] Human Rights Act 1998 ('HRA 1998').

> (b) any person certain of whose functions are *functions of a public nature*, but does not include either House of Parliament or a person exercising functions in connection with proceedings in Parliament.[419]

Section 6 further clarifies that persons do not become a public authority by virtue of undertaking a function of a public nature if 'the nature of the act is private'.[420]

'Functions of a public nature', as used in the HRA 1998, has been narrowly interpreted by the courts. In *YL v Birmingham City Council*, the House of Lords determined that a private care home was *not* carrying out 'functions of a public nature', because its functions were in pursuance to private law contractual obligations, as '[it] is necessary to look also at the reason why the person in question, whether an individual or corporate, is carrying out those activities.'[421] Thus the purposes for action must be 'public'. However, what precisely does a 'public' purpose mean in this context?

Lord Mance explained that the care home's functions were private, and to be distinguished from functions of a public nature because whereas the latter involve a 'statutory source or underpinning for its operations' the former arises out of an 'essentially contractual source' even if it is 'a matter of public concern and interest'.[422] This would mean that functions of a public nature must be mandated by statute which imposes a restrictive view of the terminology. In agreement with this, Lord Neuberger considered that the HRA 1998, 'Section 6(3)(b) is primarily concerned with functions and what is entailed with them (e.g. statutory powers and duties) rather than to whom they are provided, or indeed who provides them.'[423] Furthermore, 'The fact that a service can fairly be said to be to the public benefit cannot mean, as a matter of language, that it follows that providing the service itself is a function of a public nature'. [424] Could a similarly restrictive interpretation be extrapolated to the interpretation of 'public nature' in paragraph 5(d)?

---

[419] HRA 1998, s 6(3)(a)-(b) (emphasis added).
[420] HRA 1998, s 6(5).
[421] *YL v Birmingham City Council* [2007] UKHL 27 [31] (Lord Scott).
[422] ibid [120] (Lord Mance).
[423] ibid [165] (Lord Neuberger).
[424] ibid [135] (Lord Neuberger).

The significant criticism in the literature[425] which followed *YL* is worth mentioning here (as is the fact that Parliament specifically abrogated the part of the ruling that held a private care home was not exercising functions of a public nature)[426]. Critics of *YL* generally question 'The conceptual coherence of the division [between private and public bodies] ... when private bodies are deeply involved in fulfilling the responsibility of government through the provision of public services.'[427] As advocated by the minority in *YL* (Lord Bingham and Baroness Hale), a purposive approach is required to assess whether a function is 'public', looking to the intention behind the function; in *YL* the minority stated:

> The intention of Parliament is that residential care should be provided, but the means of doing so is treated as, in itself, unimportant. By one means or another the function of providing residential care is one which must be performed. For this reason also the detailed contractual arrangements between Birmingham, Southern Cross and Mrs YL and her daughter are a matter of little or no moment.[428]

The minority placed far more weight on the 'how' and 'why' a function is carried out, whereas the majority focused on the question of 'who'. Given that Parliament subsequently amended the law (in section 73 of the Care Act 2014) to reflect the minority's view point, what might this mean for a broader interpretation of the 'public nature' under paragraph 5(d)?

First, outside of *YL*, there is no direct authority on the meaning of this term for the purposes of paragraph 5(d). In support of a broader interpretation than provided by the majority in *YL*, it is crucial to consider that Schedule 2 provides standalone provisions to justify the processing of personal data pursuant to statutory powers and duties in paragraphs 5(b) and 5(c).[429] Indeed Lord Mostyn raised this specific point with

---

[425] Stephanie Palmer, 'Public Functions and Private Services: A Gap in Human Rights Protection' (2008) 6 International Journal of Constitutional Law 585; Alexander Williams, 'YL v Birmingham City Council: Contracting out and "Functions of a Public Nature"' (2008) 4 European Human Rights Law Review 524; Donnelly Catherine, 'Privatization and Welfare: A Comparative Perspective' (2011) 5 Law & Ethics of Human Rights 337.
[426] Reflected in the Care Act 2014, s 73.
[427] Palmer (n 425) 598.
[428] *YL* (n 421) [16] (Lord Bingham).
[429] Rosemary Jay submits that Sch 2, para 5 and the scope of its provisions, refer to 'processing carried out under a discretionary power rather than a legal obligation'. The Scottish Government in its guidance on data sharing in the public sector provides that para 5(b) encompasses processing 'that is

regard to paragraph 5(d) in order to distinguish its scope from the other provisions within paragraph 5.[430] If the public interest condition is to have any independent meaning from 5(b) or 5(c) (which Lord Mostyn's brief discussion indicates it has) functions of a public nature would need to encompass processing *outside* explicit statutory powers and duties. Certainly, if considering the legislative history to the DPD, all discussions regarding the public interest provisions indicate a distinct separation between justification based on explicit statutory mandates and the public interest on the other hand.[431]

Government guidance further supports a broader interpretation of 'public nature'. For example, the Scottish Government considers paragraph 5(d) as encompassing processing that 'is not carried out pursuant to express or implied statutory functions or as part of the functions of the Crown, a Minister of the Crown or a government department'.[432] The Ministry of Justice's guidance on data sharing would similarly support this broader interpretation.[433] What little guidance exists presupposes that processing of a public nature is processing aimed at some sort of 'public' benefit, as opposed to a solely private benefit. Even though this is not explicitly provided for in guidance or case law, it is likely that processing would need to be undertaken with the *purpose* of benefiting the 'public' to be considered of a 'public nature'. It is less certain whether and if it is sufficient to allege an intended benefit to the public as a non-descript whole i.e. the population of the UK, or that data controllers must demonstrate specific and tangible benefits such as to their constituency or service users. The critical point being made here is that to be considered of a 'public nature', processing cannot be undertaken for the sole purpose of private benefit.

---

carried out pursuant to express statutory powers or that is reasonably required or ancillary to the exercise of express or implied statutory functions', whereas para 5(c) refers to processing 'relating to functions carried out by central government departments and the Scottish Ministers that derive from the Crown's common law, prerogative or statutory powers'. Jay (n 27) 215; Scottish Executive (n 416) 29–30.

430 HL Deb 23 February 1998, vol 586, col 28gc.

431 Article 7(c) in the DPD provides a justification for processing based on the legal obligations of the data controller and the second clause of Article 7(e) separately provides justification based on the 'exercise of official authority vested in the controller or in a third party to whom the data are disclosed'.

432 Scottish Executive (n 416) 30.

433 Ministry of Justice (n 417) 16.

In summary, without a clear authority on the meaning of 'public nature' it remains uncertain the extent to which the *purposes* for processing must be 'public' and precisely *how much benefit* to the public must be pursued by the processing. It is even more confusing if we consider the fourth element of paragraph 5(d) which provides that the condition can be satisfied and relied upon by 'any person'. 'Public nature' is clearly intended to act as another safeguard, such that data controllers can only rely on paragraph 5(d) if their processing is compliant with this and the other requirements. However, even if we accept that 'who' processes the data is less important than the 'how' and 'why', there is simply no guidance on how the public nature of processing is to be objectively assessed. What is the threshold that must be met for processing to be determined as 'sufficiently' of a public nature? Does processing of a 'public nature' mean that the processing must be intended to benefit the public in some way? If public nature is tied to an idea of public benefit, how does this relate to the 'public interest' in processing, if the public interest is also about conferring a benefit in the interests of the public?

3.1.3 Is the processing 'in the public interest'?

The third element to consider is whether processing is 'in the public interest'. As the analysis below will reveal, the scope and meaning of the public interest in the context of the conditions for processing remains entirely unsubstantiated. The meaning of the public interest in the conditions for processing is undefined and it was not elaborated upon by the UK Parliament while drafting the DPA 1998.[434] Consideration of the first two elements – that processing be 'necessary' and an exercise of a function in the 'public nature' – partially aids the interpretation of this question in terms of *eliminating* forms of processing that would not meet the safeguarding requirements of paragraph 5(d). Processing could not be justified by the public interest condition if the use of ordinary personal data was merely convenient for or advantageous to the data controller when other means of processing which were less intrusive and risky (such as using anonymised data) could achieve the intended aim. Furthermore, it is unlikely that processing would meet the 'public nature' threshold if it was serving a 'private' aim

[434] Discussion is limited to the broad purpose of paragraph 5(d) and not focused on substantively defining the 'public interest'. HL Deb 23 February 1998, vol 586, col 28gc.

and purpose, with an intended outcome solely or mainly for the benefit of the data controller.

Thus, while the interpretation of both 'necessary' and 'public nature' can help *eliminate* processing by procedure, it offers no aid to interpreting what is meant *substantively* by the public interest in paragraph 5(d). Significant questions of substance remain:

How does the 'public interest' relate to the 'public nature' of processing if the latter also revolves around 'publicness' as it relates to the 'how' and 'why' of processing?

If the public nature of processing is assessed in terms of the *benefits* to be accrued as a result, how does this impact upon an assessment of the public interest in processing which could also reasonably be interpreted in light 'public' benefits?

In terms of *which* 'public' should benefit from the processing, how 'public' does the public interest have to be, meaning, how *shared* are 'public' interests and how is this to be assessed?

Subsequent amendments to the DPA 1998 provide specific examples of processing which may be considered in the public interest but answers to questions regarding the substance of the 'public interest' concept remain lacking. These amendments are now considered.

3.1.3.A The DPPSPD 2000

Several examples of public interest processing were provided in the amendment of the DPA 1998 with the introduction of the DPPSPD 2000. The Schedule to the DPPSPD 2000 introduced several new conditions for processing *sensitive* personal data on the basis that such processing serves the 'substantial' public interest. These were adopted on the basis of Article 8(4) of the DPD which permits Member States to create derogations from the conditions for processing otherwise included in Article 8:

> Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.[435]

[435] DPD, Art 8(4).

Importantly, Article 8(4) of the DPD provides that the processing of special categories of personal data based on the substantial public interest must be contingent on the provision of 'suitable safeguards'. The practical effect of this is that it is not enough for the processing to be 'in the substantial public interest' but for there to also be provision of suitable safeguards.

Under the DPPSPD 2000, specific forms of processing sensitive data would now be justifiable and may be considered as examples of processing in the 'substantial' public interest:

- To prevent or detect unlawful acts;[436]
- To protect members of the public from malpractice, dishonesty or acts of maladministration;[437]
- To disclose data for the 'special purposes' regarding the commission of a crime, revealing dishonesty, etc. if the data controller reasonably believes that disclosure is in the public interest;[438]
- To facilitate confidential counselling or advice and support services;[439]
- For research purposes.[440]

Not all the conditions added by the DPPSPD 2000 are explicitly based upon the substantial public interest. Nevertheless, the specific processing types included, such as for insurance[441] and equal opportunity purposes,[442] were clearly important enough to warrant explicit justification. It is worth recalling the lobbying efforts of Member States on precisely this point and the role the public interest provisions played to address concerns over processing for various 'important' purposes. Note that at least one provision in the DPPSPD 2000 (not conditioned on the substantial public interest), regarding the processing of sensitive data for the political canvassing, was specifically lobbied for by the UK to be included as a 'public interest' in the DPD.[443]

---

436 DPPSPD 2000, Sch, para 1.
437 ibid Sch, para 2.
438 ibid, Sch, para 3. This provision refers to disclosing data for the 'special purposes' as defined in s 3 of the DPA 1998. Special purposes include processing for journalistic, artistic and literary purposes.
439 ibid, Sch, para 4.
440 ibid, Sch, para 9.
441 DPPSPD 2000, Sch, para 5.
442 ibid, Sch, para 7.
443 See Section 2.6 above. 'Note from Presidency to Internal Market Council' 11581/94, 5; Council of the European Union, 'Report, from Permanent Representatives Committee, on 10 January 1995, to Council meeting (General Affairs), on 6 and 7 February 1995' 4649/95, 2.

Processing for research[444] was also lobbied for by the UK (among other delegations)[445] and this was included in the DPPSPD 2000 as processing conditioned on the substantial public interest. Given the focus in this thesis on processing for research purposes, it is worth examining in closer detail this provision. What substantive difference is there, if any, between processing ordinary personal data based on the public interest in paragraph 5(d) versus processing sensitive personal data in the 'substantial' public interest under the DPPSPD 2000?

Research in the 'substantial' public interest

'Research' (which is defined in the DPA 1998 to broadly include statistical or historical purposes[446]) requiring the use of sensitive personal data was provided a separate legal basis for processing in the DPPSPD 2000. Under this provision, sensitive personal data can be lawfully processed for research if it is in the 'substantial public interest', and suitable safeguards are provided:

> The processing—
> (a) is in the substantial public interest;
> (b) is necessary for research purposes (which expression shall have the same meaning as in section 33 of the Act);
> (c) does not support measures or decisions with respect to any particular data subject otherwise than with the explicit consent of that data subject; and
> (d) does not cause, nor is likely to cause, substantial damage or substantial distress to the data subject or any other person.[447]

'Substantial public interest' is not defined in the DPPSPD 2000, however this terminology mirrors the DPD's Article 8(4).[448] Although 'substantial public interest' is not 'novel' to the DPA 1998, as discussed at length in Section 2 above, there are no factors discussed by Member States in the *travaux* that would help to distinguish

[444] Note, that processing for medical purposes, including for medical research, was already provided a justification in the main text of the DPA 1998, Sch 3, para 8. Research, more generally, was given justification with the adoption of the DPPSPD 2000, para 9.
[445] See Section 2.6.1 above.
[446] DPA 1998, s 33.
[447] DPPSPD 2000, para 9.
[448] DPD, Art 8(4) (emphasis added).

between 'substantial'[449] public interests and *ordinary* public interests for the purposes of processing ordinary personal data.

The most reasonable interpretation is this: given that only *substantial* public interests can justify the processing of *sensitive* personal data (versus public interests which can justify the processing of *ordinary* personal data) the term 'substantial' merely indicates the generally higher threshold for processing *sensitive* personal data. Indeed, the lawfulness of paragraph 9 (and any of the other derogations represented within the DPPSPD 2000) are contingent upon *suitable safeguards* being provided as required by Article 8(4) of the DPD. Paragraph 9's requirements b-d set forth above, represent the safeguards required by Article 8(4) of the DPD, while the requirement that processing must be in the 'substantial public interest' appears to be little more than a restatement of the requirement set out in Article 8(4). '

To further understand what if any *substantive* difference there is between research in the 'public interest' versus in the 'substantial public interest', consider the explanatory notes to the DPPSPD 2000. Although explanatory notes to UK legislation are not legally binding, the term 'substantial public interest' is not defined and therefore this explanation can be used to interpret the provision.[450] The notes provide an example of research considered to be in the 'substantial' public interest:

> Paragraph 9 of the Schedule covers, for example, processing in the course of maintaining archives where the sensitive personal data are not used to take decisions about any person without their consent and no substantial damage or distress is caused to any person by the keeping of those data.[451]

Here the maintenance of an archive is an example of processing that is 'in the substantial public interest'. The crucial focus is *not* on the substance of this example

---

[449] To add further inconsistency, the explanatory recital to Article 8(4) speaks of 'important' public interests, not substantial ones.
[450] In *R (Westminster CC) v NASS* [2002] UKHL 38, it was considered 'whether in aid of the interpretation of a statute the court may take into account the Explanatory Notes and, if so, to what extent'. In Lord Steyn's judgment, it was held that '... insofar as the Explanatory Notes cast light on the objective setting or contextual scene of the statute, and the mischief at which it is aimed, such materials are therefore always admissible aids to construction. They may be admitted for what logical value they have'.
[451] DPPSPD 2000, Explanatory Notes.

(i.e. the type of the research provided). Rather, the emphasis is on the safeguarding requirements of paragraph 9: that the processing is not used to take decisions about individuals without their consent and that no substantial damage or distress is caused to individuals by archiving data. Thus, we see again (as with 'necessary' and 'public nature' for paragraph 5(d)) the emphasis on safeguards, which if not provided, would eliminate processing from being considered in the 'substantial' public interest. The explanatory notes reinforce the interpretation suggested above; that the 'substantial' public interest terminology reveals little about the substantive parameters for determining what is in the substantial public interest and more about the type of data at issue and the required safeguards for processing per Article 8(4) of the DPD. We lack objective criteria to positively determine what can be considered processing in the 'substantial' public interest as this higher public interest threshold is not further explained.

Although examples of processing in the substantial public interest are provided in the DPPSPD 2000, which could also arguably meet the elusive 'public interest' threshold for ordinary personal data[452], we still lack the ability to substantively assess whether processing which is *not* explicitly mentioned, is or is not in the public interest. Even if the enumeration of specific 'substantial' public interest examples in the DPPSPD 2000 seem to indicate an *exhaustive* list of 'substantial' public interests for the purposes of processing *sensitive* personal data (*expressio unius est exclusio alterius*),[453] the same cannot be said about paragraph 5(d) as to ordinary personal data, which is an open-ended provision.[454] This brings us back to the question of what precisely does the public interest mean in context with processing personal data – what processing purposes are 'public' enough and what 'interests' are encapsulated by these provisions aside from the explicit examples provided?

---

[452] Subject to the requirements of 'necessary' and 'public nature' in the DPA 1998 Sch 2 para 5(d).
[453] However, if we read the DPPSPD 2000 *purposively* and in line with the intended purpose and scope for the equivalent provisions in the DPD, Article 8(4) and Recital 34 were *not* drafted to provide an exhaustive list of 'substantial' public interests.
[454] In the case of Sch 2 para 5(d), no examples of the 'public interest' are provided. Furthermore, the use of the term 'any' ('for the exercise of *any* other functions of a public nature exercised in the public interest by *any* person') indicates the open nature of the provision as opposed to the specific, enumerated list of 'substantial' public interests in the DPPSPD 2000. This interpretation is supported by the Parliamentary discussions on the provision and moreover by a purposive reading which should reflect the non-exhaustive nature of the equivalent provisions in the DPD.

3.1.4 Processing by 'any person'

The fourth and final element of paragraph 5(d) is not necessarily one to be satisfied, but instead is a device to support the interpretation of another requirement – that processing be related to the undertaking of functions of a *public nature*. As discussed above, paragraph 5 distinguishes between processing 'in the public interest' and processing justified based on serving official statutory functions and obligations. Thus, the main elements of the public interest condition are: 1) that the processing is necessary; 2) related to functions of a public nature and 3) in the public interest. The fact that the provision can be satisfied by 'any person' merely permits that, for example, quasi-public organisations or voluntary organisations, could meet these requirements.[455] Moreover, the use of the term 'any person' is indicative of the broader purposes of this provision, not confined or restricted to specific examples as *may* be the case with sensitive personal data under the DPPSPD 2000,[456] or indeed by the restrictive ruling on 'public nature' by the House of Lords in *YL*.

3.2 Interim conclusion on the public interest conditions

The public interest conditions seemingly focus on the *proportionality*, *'publicness'* and *safeguarding* of processing. Does the public interest being served require the use of personal data, or would anonymised data suffice ('necessary')? Furthermore, does the purpose for processing arise out of a typically public function and is the purpose for processing intended to benefit the 'public' or is it predominantly for private gain ('public nature')? If sensitive personal data are being used, will decisions be taken based on such processing, without the consent of individuals, or is the processing likely to cause great harm or distress to anyone? While these requirements can certainly *eliminate* certain circumstances of processing where sufficient safeguards are not provided to individuals, a key element – that that the processing must be 'in the public interest' (or 'substantial' public interest for sensitive personal data) – remains uncertain in scope and undefined.

[455] Ministry of Justice (n 417) 16.
[456] See note 454.

In summary, while the DPA 1998 does indeed provide safeguards to individuals where the public interest is relied upon to justify processing of personal or sensitive personal data,[457] the public interest conditions do not ultimately resolve the uncertainty regarding the substantive meaning of the concept. The required 'publicness' of the 'public interest' and what 'interests' may meet this threshold remains uncertain. Understanding these components are crucial to assessing whether a given form of processing is sufficiently in the public interest to satisfy these conditions. Given the use of the term 'public interest', and in understanding the purpose behind the provisions in considering the legislative history of the DPD and DPA 1998, it cannot be that mere procedure qualifies a given form of processing as 'in the public interest'. In other words, data controllers must be able to substantiate *more* than just that their use of personal data is 'necessary' and of a 'public nature'. The public interest conditions in the DPA 1998 require data controllers to establish that their processing is in the public interest, but currently, they are without a means for doing so.

4. Conclusion

In this chapter, we have considered the long and protracted legislative history of the DPD to examine the purposes for including the public interest provisions within the Directive and to better understand the provisions' intended role and scope. The *travaux* do reveal the intended purposes for the public interest provisions – to legitimise certain important forms of processing where consent cannot be obtained. The provisions arose out of the concerns of many delegations regarding the chilling effect of the Directive on certain forms of data processing, such as research. The public interest provisions developed into a 'compromise' where these forms of processing were not fully exempt or excluded from the Directive but could proceed 'unimpeded', mainly meaning that consent would not be required. Although we get a sense of the types of processing that could meet the requisite 'public interest' threshold, through the lobbying efforts of Member States, and the eventual inclusion of these lobbied for processing types in Recital 34 of the Directive, no objective criteria are provided to facilitate data controllers' assessment of the public interest in their processing.

[457] Per DPD, Recital 34 and Article 8(4).

The DPA 1998, and the transposition of the public interest provisions into the legal conditions for processing in Schedules 2 and 3, were then examined to determine whether these uncertainties were resolved and what safeguards were provided when the public interest would be relied upon to justify processing. Safeguards are indeed embedded within the public interest condition for processing ordinary personal data in Schedule 2 paragraph 5(d). Under this condition, the processing of ordinary personal data is lawful so long as it is necessary, related to a function of a public nature and in the public interest; this justification is not limited to public authorities but can be satisfied by 'any person'.[458] As to the processing of sensitive personal data, specific provisions were later added which justified processing based on the 'substantial' public interest. Although examples of processing in the 'substantial' public interest are provided, such as processing for research, the focus of the provisions remains on the safeguards (e.g. not taking decisions based on processing and ensuring no harm or distress will occur as a result) as opposed to the public interests at stake.

The safeguards built into the public interest conditions do assist in eliminating certain processing circumstances which could not be considered in the public interest. However, satisfying the safeguarding requirements of the public interest provisions simply does not indicate whether processing is *substantively* in the public interest. The effect of this has been that data controllers are without relevant guidance to determine whether a given form of processing is in the public interest or not, unless it is one of the types explicitly mentioned in the DPPSPD 2000 or the DPD. Even where a type of processing *is* specifically mentioned, the predominance of consent or anonymisation indicates that the public interest provisions are not routinely being relied upon, and arguably this is due to this lack of definition and consequent uncertainty.[459] Furthermore, in light of the insight gained from my analysis of the *travaux*, it is highly unlikely that merely because a type of processing is mentioned as an example in the DPD, that this automatically qualifies it as justifiable 'in the public interest' in a normative sense.

---

[458] DPA 1998, Sch 2, para 5(d).
[459] See Chapter 2 Section 2.2 and 4.

While it is admittedly an impossible task to define exhaustively every possible form of public interest processing, it is my contention that that the public interest conditions in the DPA 1998 and DPD require data controllers to substantiate and establish *more* than just their compliance with the required safeguards. If the opposite were true, this would mean the public interest is an empty term. Public interest processing would mean nothing more than the sum of its procedural parts – that if processing is 'necessary' and of a 'public nature' with the appropriate safeguards in place, it is in the public interest. However, processing arising out of public functions and obligations are dealt with separately in both the DPA 1998 and DPD,[460] and in light of the extensive discussion delineating the broader purposes for the public interest provisions in the *travaux* of the Directive, it is far from likely that this was the intention.[461] As the *travaux* of the Directive also make clear, the task of further refining the public interest provisions was left to Member States.[462] As seen by examining the DPA 1998 and related guidance, this task has not been undertaken.

In Chapter 4 I explore whether it is possible to more clearly define the public interest in a *substantive* and thus normative sense, beyond mere procedure. To do this, I expand the legal evidence base on the operation of the public interest by considering how the concept is interpreted in context with Article 8 of the ECHR, given the frequent overlap with data protection claims.

---

460 In the DPA 1998, Sch 2, para 5(b)-(c); and the DPD, Art 7(c) and second phrase in Art 7(e) which provides that 'processing is necessary for the performance of a task carried out in the public interest *or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed*' (emphasis added).

461 See Section 2.6 above.

462 'Note, from Presidency, 14 April 1994, for Working Party on Economic Questions (Data Protection)' 6316/94, 3; 'Note, from Presidency, 10 May 1994, to Permanent Representatives Committee' 6856/94, 12.

Chapter 4 Reviving the Public Interest Concept in Data Protection Law

1. Introduction

The public interest conditions for processing require data controllers to engage with the *substantive* meaning of the public interest but, as discussed in Chapter 3, the law fails to provide any basis for doing so. The *travuax préparatoires* revealed that the types of data processing included as examples of data use in the public interest, such as medical research, were no more than the result of political negotiation. The *travaux* further indicated that these are merely examples and do not represent an exhaustive list of the types of processing that can be justified in the public interest. Without the provision of criteria or other means for assessing the public interest in processing, it remains entirely unclear what the public interest can mean in a substantive sense in this context. Therefore, the purpose of this chapter is to develop a deeper conceptual understanding of what the public interest means in data protection and consider how we might define the concept in a *substantive* and thus normative sense, beyond mere procedure.

To emphasise the task at hand, the chapter begins by first considering why, on a conceptual level, it is difficult to define the public interest. By adopting W B Gallie's concept of 'essential contestability'[463] I outline reasons why defining the public interest is problematic in the data protection context. This provides the appropriate backdrop for later assessing current understandings of the public interest within the law.

I follow this with an overview of what is understood as 'the public interest' under the current legal framework. From the analysis in Chapter 3, this includes the 'list' of various types of processing which are examples of the public interest enumerated under the DPD and DPA 1998. To further our understanding of the public interest concept, I expand this list of public interests to include those from Article 8 of the ECHR, given

[463] Gallie (n 49) 169.

the common overlap of Article 8 and data protection claims. I consider what Article 8 jurisprudence can offer in terms of explaining the substantive meaning of the public interest, in context with the conditions for processing in data protection. While this analysis offers insight on the safeguarding aspects of the public interest conditions, ultimately, only a descriptive understanding of the public interest remains without any criteria which could be applied objectively and consistently to different processing circumstances.

The next part of the chapter draws upon political and legal theory to fill the conceptual gaps identified from the legal analysis on the public interest in data protection and Article 8 jurisprudence. I use theory to interrogate the legal iterations of the public interest to determine 1) the appropriate conceptual boundaries of the concept and 2) what criteria may be relevant to assessing whether the processing of personal data is justified in the public interest. Combining this legal and theoretical analysis reveals key components to reframe our consideration of the public interest concept in a way that improves upon current understandings and practices in data protection.

2. The Difficultly in Defining the Public Interest: The Essential Contestability of the Concept

Why is it so difficult to define the public interest? Since the enactment of the DPD and the DPA 1998, the concept has received relatively little critical attention. This being said, the insight that has been offered from law[464] and other disciplines[465] often focus on the ambiguity of the concept. As such, theoretical development and understanding of the concept as it is used in data protection is lacking. Why is it difficult to delineate the types of processing or circumstances in which it is justifiable to rely on the public interest? The key theoretical issues or typical 'pitfalls' of relying upon the public interest concept are articulated in Jane Mansbridge's work on the public good (a term she uses synonymously with the public interest).[466] Mansbridge presents three vulnerabilities of the public interest concept:

[464] McHarg (n 28) 671, 674; Townend (n 28); Beyleveld (n 28); Taylor (n 28).
[465] Bozeman (n 59).
[466] Mansbridge (n 49).

- The public interest is an *essentially contested concept*[467]*:* We can never know in advance and with certainty what the public interest is in any given case[468] and this is most unsettling in the legal context given the normative weight of legal decisions and judgments.
- The public interest is vulnerable to *demagogic exploitation*: Dangers lurk in the emotional bases of appeals to the public interest, which are associated with historical examples that demonstrate various and nefarious motives couched in public interest terminology. These undermine further appeals to the concept.[469]
- The public interest is vulnerable to *control by dominant groups*: Given the ambiguity of the concept, dominant and elite sectors of society have the advantage to construct reigning understanding of the public interest to the disadvantage of other groups.[470]

It is the public interest's essentially contested nature, its uncertainty in any given context, and its susceptibility to exploitation by a decision maker that make the concept 'suspect' when used as a justification for action in any context, but especially in data protection where such decisions and reasoning are made in *private* and are not currently subject to public scrutiny.[471] (Currently, data controllers may independently determine their processing is justifiable based on the public interest without any scrutiny, legal or otherwise.) Exploring the idea of 'essential contestability' as it applies to the public interest illustrates the complexity involved when attempting to define it and therefore the issues that arise when attempting to use the concept in a legal context. W B Gallie introduced 'essential contestability' in 1955, to explain 'concepts the proper use of which inevitably involves endless disputes about their proper uses on the part of their users.'[472] Gallie defines essentially contested concepts according to four criteria:

- *Appraisive*: 'it signifies or accredits some kind of valued achievement';
- *Internally complex*: 'achievement must be of an internally complex character, for all that its worth is attributed to it as a whole';
- *Variously describable* (i.e. *component features are in dispute*): 'explanation of its worth must therefore include reference to the respective contributions of its various parts or features';

---

467 Mansbridge and other theorists used W B Gallie's concept of 'essential contestability' to analyse the public interest. Gallie (n 49) 168–169; Mansbridge (n 49); O'Flynn (n 49).
468 Mansbridge (n 49) 4.
469 On this Mansbridge explains: 'Yet, after Hitler and Freud, the present generation's heightened sensitivity to the dangers of drawing on the emotions tends to undermine appeals to public spirit or the public good.' ibid 4–5.
470 ibid 5.
471 ibid.
472 Gallie (n 49) 169.

- *An achievement subject to change over time*: 'accredited achievement must be of a kind that admits of considerable modification in the light of changing circumstances; and such modification cannot be prescribed or predicted in advance.'[473]

The public interest, when used in data protection, is indeed an *appraisive* concept, intended to signify a valued achievement pursued by the data controller e.g. processing data on behalf of public health or social protection.

The value or achievement associated with the public interest in data protection is *internally complex* given the contextual nature of the concept and vast subject matter it can represent – any innumerable types of data processing as well as the protection of informational privacy. This complexity is particularly difficult to grapple with in making legal decisions given the demands of the Rule of Law in terms of 1) generality; 2) public accessibility; 3) prospective quality; 4) intelligibility; 5) consistency; 6) practicability; 7) stability and 8) congruency between rules and their administration.[474] As it stands, the public interest concept, as used in the conditions for processing, fails on all these counts.

The public interest's various *component features remain in dispute*, with rival conceptions revolving around the following questions: In *whose* interest? What public or publics are relevant? How do we ensure those interests are representative of the 'public' and not of the self-interest of the decision-makers? At least three theories claim to define the core features of the public interest and offer the 'true' meaning of the concept, yet no single theory dominates in data protection.[475]

Finally, understandings of the public interest are necessarily contextual matters, *subject to change over time* and dependent upon the relevant public(s) in question.[476]

---

[473] ibid 171–172 (emphasis added).
[474] Lon L Fuller, *The Morality of Law* (Revised Edition, YUP) 39.
[475] This would include preponderance theories, common interest theories and unitary theories of the public interest, examined in Section 4 below.
[476] Fifth and sixth elements were convincingly disregarded by Waldron as unnecessary to maintain the essential contestability of a concept, these were: (5) the previous existence of an exemplar of the concept and (6) awareness by those who use the concept, of its essential contestability. Gallie (n 49)

The essential contestability of the public interest[477] undoubtedly presents difficulties in making *justifiable* legal decisions. The ambiguity surrounding the public interest challenges the legal agenda, which presumes and relies upon facts being 'knowable' and amenable to making concrete, legal decisions. Furthermore, legal decisions justified in the public interest are likely to be attacked not only because of the ambiguity of the concept, but because of how such decisions are arrived at – suspicion of self-interest being masked as 'the public interest'. Nevertheless, it is in fact this 'contestation between rival conceptions [that] deepens and enriches our sense of what is at stake in a given area of value.'[478] The uncertainty that surrounds the public interest and that which makes it problematic in the data protection context invites a level of dialogue that is necessary to affect a 'marked raising of the level of quality of arguments in the disputes of the contestant parties.'[479]

Problematically, such dialogue has not been happening within the data protection context, a point which will be addressed in Chapter 6 when recommendations are made for improving current practices around public engagement. Furthermore, while legitimate decision making procedures are clearly required to decide in matters of conflict between the use of personal data and the protection informational privacy, this must be based upon *some* understanding of the range of circumstances in which processing is justifiable 'in the public interest'. This requires an understanding of what the public interest means on a conceptual level and thus what criteria can be used to assess the public interest in processing to determine *when* processing is justifiable in a normative sense: When is processing justified in the public interest *despite* any conflicts with the public (and private) interests in protecting informational privacy and any other interests opposed to processing?

171–172; Jeremy Waldron, 'Is the Rule of Law an Essentially Contested Concept (In Florida)?' (2002) 21 Law and Philosophy 137, 158–160.

[477] Also considered by: Mansbridge (n 49).

[478] Waldron (n 476) 162.

[479] Gallie (n 49) 193.

In the section below I consider how the public interest concept is currently understood in the law revealing the conceptual gaps that must be filled to achieve an improved understanding and more legitimate deployment of the public interest in data protection.

3. Legal Understandings of the Public Interest

Currently in data protection law, to determine whether a given form of processing is justifiable in the public interest, one would need to take account of:

- The safeguarding requirements of the public interest conditions: that the processing is 'necessary' and related to a function of a 'public nature';[480]
- The 'list' of public interests provided under the DPD and DPA 1998 as to the processing of sensitive personal data.[481]

While considering whether the processing of personal data is 'necessary' or sufficiently of a 'public nature' are far from straightforward tasks, there are simply *no* criteria for determining what types of processing are 'in the public interest'. What processing purposes are 'public' enough and what 'interests' are encapsulated by the public interest provisions?

As examined in Chapter 3, the DPD provides a legal justification for the processing of personal and 'special categories' of personal data based on the public interest.[482] The DPD provides more explicit detail (in the Recitals) as to what types of processing may be justified based on the public interest when processing special categories of personal data (sensitive data in the UK), which analysis of the *travaux* revealed, also applies to ordinary personal data[483]:

---

[480] Which has been interpreted in the UK in line with the meaning of 'necessary' in context of Article 8 ECHR jurisprudence. For example: *Daly* (n 85) [26]-[27]; *Ellis* (n 85) [1], [27]-[29]; *Stone* (n 85) [60] (Davis J); *Corporate Officer* (n 85) [59].

[481] DPD, Recitals 34-36.

[482] DPD, Article 7(e) provides legal justification for processing personal data where the '…processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed'. As to sensitive personal data, the DPD Article 8(4), when read in conjunction with the associated Recitals 32, 34-36, provides more explicit grounds of 'important' public interest which would justify the processing of special categories of personal data ('sensitive data' under the DPA 1998).

[483] 'Extract from the Draft Summary Record of the 1628th meeting of the Permanent Representatives Committee Part 1 held in Brussels on 14 November 1994' 10957/94, 9: 'The Council and the Commission note that the elements set out in recital 17a of the Directive, which are intended in

> Whereas Member States must also be authorized, when justified by grounds of important public interest, to derogate from the prohibition on processing sensitive categories of data where important reasons of public interest so justify in areas such as *public health* and *social protection* - especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system - *scientific research* and *government statistics*; whereas it is incumbent on them, however, to provide specific and suitable safeguards so as to protect the fundamental rights and the privacy of individuals.[484]

This 'list' of potential public interest uses also includes:

> Whereas, moreover, the processing of personal data by official authorities for *achieving aims, laid down in constitutional law or international public law, of officially recognized religious associations* is carried out on important grounds of public interest;[485]
>
> Whereas, in the course of *electoral activities*, the operation of the democratic system requires in certain Member States that political parties *compile data on people's political opinion*, the processing of such data may be permitted for reasons of important public interest, provided that appropriate safeguards are established.[486]

Therefore, the DPD presents a *descriptive* understanding of the public interest processing, meaning the public interest is defined only by reference to the following examples:

- public health;
- social protection;
- scientific research;
- government statistics;
- membership records of officially recognised religious organisations; and
- electoral activities.

---

particular to clarify the concept of public interest in Articles 7 and 8 of the Directive, derive from the purpose of the latter and thus form an integral part of this legal act; it follows that those elements are to be taken into consideration by the Member States when they adopt the laws, regulations and administrative provisions required to comply with the Directive.' This refers to what eventually became Recital 34 of the DPD. See Chapter 3 Section 2.7.

[484] DPD, Recital 34 (emphasis added).

[485] ibid, Recital 35 (emphasis added).

[486] ibid, Recital 36 (emphasis added).

Crucially, as revealed in Chapter 3, no logical explanation is provided as to the examples' specific relationship to the public interest.[487] Investigation of the *travaux* illustrates the political agendas driving certain forms of processing to be considered 'exempt' from the full force of the Directive on grounds of public interest.[488] There were significant lobbying efforts made to include research and statistics into this broad category but no guidance is provided as to how, in specific cases, the processing of data for research or statistics could be assessed in terms of the public interest; rather, it seems that it was generally and uncritically assumed that such activities were 'clearly vital' to the public interest.[489]

Upon implementing the DPD into national data protection laws, Member States such as the UK have sought to fill these gaps on the public interest by adopting European jurisprudential principles related to cases engaging Article 8 of the ECHR. However, Article 8 is only relevant when an individual's Article 8 rights are at issue, which is *not* necessarily true in all data protection disputes. Indeed, data protection law offers a discrete right to protect an individual's personal data, which is separate from (although potentially overlapping with) that same person's right to private and family life under Article 8 of the ECHR.[490] Nevertheless, Article 8 provides its own 'list' of public interest examples, which are relevant to examine and expand our understanding of the public interest at work where there *is* overlap between data protection law and the ECHR.

---

[487] See Chapter 3 Section 2.6.

[488] For example, with the lobbying efforts to exempt the processing of personal data for research by the UK, Ireland, Greece, Denmark, Belgium, Spain, the Netherlands, and Italy. See Chapter 3 Section 2.6.1 - 2.6.1.C.

[489] For example, in regards to the processing of personal data for statistical purposes, the German Presidency of the Council of the EU provided 'Processing undertaken for the purpose of compiling statistics in the public interest - an exercise in which data subjects are obliged to take part - within the framework of programmes being implemented by the national statistical offices *is obviously regarded as a task in the public interest*.' Whereas the justification of processing data for research purposes is based on the assumption that such research is of 'major importance to society as a whole.' 'Working Document, from Presidency, concerning statistics/scientific research problems, 20 July 1994' 8525/94, 3 (emphasis added).

[490] As I have considered elsewhere: Black and Stevens (n 11) 108–109.

3.1 The public interest under Article 8 of the ECHR

Given the overlap between notions of data protection and the right to respect for private life conferred by Article 8 of the ECHR, Member States have deferred to the European Court of Human Rights ('ECtHR') and its interpretation of key terms which apply in both legal contexts.[491] The ECtHR's interpretation of Article 8 provides other potential meanings of the public interest concept in the context of data processing and has strongly influenced the UK's interpretation of terms within the DPA 1998, notably the meaning of 'necessary' within the conditions for processing and its relationship with the principle of proportionality.[492] The analysis below considers the 'list' of public interests which may be considered 'legitimate' interferences with an individual's Article 8 rights and the associated procedure for assessing this in each case.

3.1.1 The public interests added by Article 8

At the outset, it is important to note that the exact term 'the public interest' is *not* used in Article 8 of the ECHR. Rather, 'legitimate purposes' and 'pressing social need' are used. However, the term 'public interest' *is* used synonymously by the ECtHR in cases determining Article 8 issues, for example in *LH v Latvia*.[493] Furthermore, it is contended here that the text of Article 8 can reasonably be read to encompass the concept of 'the public interest' (or some other analogous concept) with for all practical purposes, the same meaning in data protection.

Article 8(2) sets forth a framework for deciding situations of conflict between wider, collective interests, served by a Member State and the protection of an individual's right to a private and family life.[494] Article 8 provides that an individual's right to private and family life are not to be interfered with by a Member State unless it is:

---

[491] For example, in the UK: *Daly* (n 85) [26]-[27]; *Ellis* (n 85) [1], [27]-[29]; *Stone* (n 85) [60]; *Corporate Officer* (n 85) [59]; *Catt* (n 85) [6]; *AB* (n 85).
[492] See Chapter 3 Section 3.1.1.
[493] Where the Republic of Latvia justifies their interference with the applicant's Article 8 rights to protect public health: as a 'provider of health care services, "with the aim of protecting public interests, is also entitled to request the assessment of the quality of medical care" in order that, should any irregularities be found, they might be eliminated and their recurrence with respect to other patients avoided in the future.' *LH v Latvia* App No 52019/07 (ECtHR, 29 July 2014), paras 34, 52.
[494] This view is supported by: McHarg (n 28); Bart van der Sloot, 'How to Assess Privacy Violations in the Age of Big Data? Analysing the Three Different Tests Developed by the ECtHR and Adding for a Fourth One' [2015] Information & Communications Technology Law 1.

> …in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[495]

Here, we see at least two examples of the public interest which overlap with those provided in the DPD: public health and social protection (listed in Article 8 as 'the protection of health', whereby 'social protection' from the DPD could be read into the provision for 'national security', 'public safety', 'prevention of disorder or crime', or 'the protection of morals'). Article 8's more detailed description of social protection indicates more broadly the types of processing that could be justifiably encompassed within the context of data protection law. Given the non-exhaustive nature of the examples of public interest processing provided in the DPD,[496] it can only be assumed that a valid meaning of the public interest (or analogous concept) in the human rights context is *also* valid under the DPD, where *informational* privacy is at stake (considering Member State's obligations under the ECHR vis-à-vis implementation of their national data protection legislation). Therefore from Article 8, we add to the 'list' of public interests introduced in above, the processing of data which serves the following purposes:

1. National security;
2. Public safety;
3. Economic wellbeing of a Member State;
4. Prevention of disorder or crime;
5. Protection of health or morals; and
6. Protection of the rights and freedoms of others.

While Article 8 uses broader language to describe these public interests, the examples provided are only descriptive and do not tell us how to assess the public interest of each case. Under the DPA 1998, the fact that processing ordinary personal data is 'in

---

495 ECHR, Article 8(2) (emphasis added).

496 As discussed in Chapter 3 Section 2.6.1.C and 2.7, the final drafting of Recital 34 of the DPD was framed as an explanatory device to guide Member State's understanding of the public interest provisions and to provide *examples* for this purpose. The examples of processing in Recital 34 were not intended to be exhaustive. 'Note, from Presidency, 14 April 1994, for Working Party on Economic Questions (Data Protection)' 6316/94, 3; 'Extract from the Draft Summary Record of the 1628th meeting of the Permanent Representatives Committee Part 1 held in Brussels on 14 November 1994' 10957/94, 9.

the public interest', is not in itself enough to justify that processing, as it must also be necessary and related to a function of a public nature. Similarly, under Article 8, the undertaking of an activity from the list above does not in itself justify an interference with an individual's rights; the Member State must also demonstrate that their actions are '[In] accordance with the law and is necessary in a democratic society.'

On the face of Article 8, we are left in the same position as under data protection law: without any means for going beyond mere description or procedure to understand how to assess and apply the public interest concept in each case. However, Article 8 is the subject to a wide body of case law, which has been used in the UK to interpret key terms within the public interest conditions of the DPA 1998. It is instructive to now examine the extent to which the European case law interpreting Article 8 can be used to develop a conceptual understanding of the public interest in data protection law.

3.1.2 The procedure of assessing the public interest in Article 8

In the context of Article 8, the validity of a Member State's claim that their interference with an individual's rights is justifiable is assessed in terms of the sufficiency of procedural guarantees provided to the person. The public interest claim is represented by 'interferences' by the State in their pursuit of achieving a 'legitimate aim'. For a Member State to not be considered in breach of their obligations under Article 8, any interference 'must be in accordance with the law and deemed necessary in a democratic society'. These requirements correspond easily with the data protection context which requires any form of processing (without consent) to be necessary and lawful, requiring general legal compliance but also adherence to a specific legal basis for processing, as provided in Articles 7 and 8 of the DPD, for personal and 'special categories' of personal data respectively.[497]

However an important distinction is that the public interest provisions under data protection law are 'positive' in that they *support* a data controller's processing in an action-promoting sense. In contrast, Article 8 cannot be said to support a Member

[497] DPD, Articles 7-8, transposed in the DPA 1998, Schs 2 and 3.

State's interference with an individual's rights; rather Article 8 prohibits such interferences unless they abide by the conditions in which they would be *defensible*: 'There *shall be no interference* by a public authority with the exercise of this right except such as…'.[498] Under data protection law, the processing of personal data is not a *de facto* interference or violation of an individual's rights *unless* it is e.g. unlawful (undertaken without a legal basis), is otherwise unfair or in breach of one of the other data protection principles. Thus the threshold for substantiating processing based on the public interest would be markedly different than that for substantiating a *de facto* interference with an individual's human rights.

Nevertheless, the UK has adopted the ECtHR's interpretation of key terms within the DPA 1998's public interest conditions (i.e. 'necessary'), making the case law of Article 8 a relevant area to examine. While it is beyond the scope of this thesis to provide an in-depth examination of Article 8 jurisprudence, what is of relevance to the aims of this thesis are the two following areas: 1) how the ECtHR has assessed the 'legitimacy' or 'public interest' of a Member State's actions and 2) how it has assessed the 'necessity' of that action *in proportion* to the public interest aim sought. These two aspects of Article 8 jurisprudence will be examined in depth below.

3.1.2.A The ECtHR's assessment of the public interest

Once the ECtHR has established that a Member State's actions have interfered with an individual's Article 8 rights,[499] the Court considers whether their actions were 'in accordance with the law'. The ECtHR would next consider whether a Member State's actions were in pursuit of a 'legitimate aim' or in other words, whether they served a legitimate public interest. This consideration receives a relatively light touch assessment, which I argue is because the relative 'public interest' of a Member State's claim is restricted to the defined set of circumstances prescribed by Article 8(2). Rather than engage in broad and conceptual considerations of what 'legitimate aim' can or

[498] ECHR, Article 8(2) (emphasis added).
[499] Which is a relatively low threshold to meet in the context of Article 8. The mere storage of personal data, regardless of whether and how data are later used, is considered enough to engage an individual's Article 8 rights. *Leander v Sweden* (1987) Series A no 116, para 48, reconfirmed in *S and Marper v The United Kingdom* App nos 30562/04 and 30566/04 (ECtHR, 4 December 2008), para 69.

cannot mean in the context of Article 8, the Court merely confirms that a Member State's actions fall within the list of public interests under Article 8. For example, in *S and Marper v the United Kingdom*, the ECtHR provided that:

> The Court agrees with the Government that the retention of fingerprint and DNA information pursues the legitimate purpose of the detection and, therefore, prevention of crime. While the original taking of this information pursues the aim of linking a particular person to the particular crime of which he or she is suspected, its retention pursues the broader purpose of assisting in the identification of future offenders.[500]

Here the ECtHR connects the legitimate aim sought by the UK to the examples of public interest provided under Article 8(2), namely the prevention of crime. This suggests a strict interpretation of the public interest under Article 8(2); that the legitimate aim sought by a Member State *must* fall within the discrete categories enumerated. Indeed, in the case of *Funke v France*, the ECtHR provided that the public interest 'exceptions' provided in Article 8(2) had to be interpreted *narrowly*.[501]

This approach would contrast with the public interest examples provided in data protection law, which as revealed in Chapter 3, were intended to be non-exhaustive. Thus, in Article 8 it seems that the substantive meaning of the public interest is specifically confined to the list of examples provided in Article 8(2). As indicated above, this is appropriate for the aims of the ECHR which focuses on protecting individuals from arbitrary interferences from Member State action. Nevertheless, Member States' actions are not justifiable solely on the basis that they serve the public interest. Rather, the Court intensely scrutinises the justifiability of a Member State's public interest claim in terms of whether their actions are lawful and necessary. Thus, under Article 8 the public interest is assessed descriptively (in terms of the examples given) *and* through procedure. Although it is my contention that data protection law requires a deeper conceptual and substantive understanding of the public interest, beyond description and procedure, analysing the operation of procedure under Article 8 case law can nonetheless reveal insights into the range of circumstances in which the public interest can justify action.

---

[500] *Marper* (n 499) para 100.
[501] *Funke v France* (1993) Series A no 256-A, para 55.

3.1.2.B 'In accordance with the law'

The ECtHR spends far more time analysing whether a Member State's actions are 'in accordance' with the law, than in their consideration of the public interest. The Article 8(2) requirement that an interference must be 'in accordance with the law' necessitates compliance with all relevant domestic and international obligations, but Member States must also demonstrate a specific lawful basis for the interference. However, this requirement is not merely about legal compliance or a lawful basis for action – 'in accordance with the law' requires the assessment of several related considerations.

- Are there safeguards provided in the law to prevent arbitrary interferences by the State?[502]
- Is the law accessible to those who would be affected by it?[503]
- Is the law sufficiently clear with predictable consequences for individuals?[504]

The legality requirement is considered with varying emphasis in each case.[505] For instance, in *Evans v the United Kingdom*, the actions of the UK were in furtherance of the protection of societal morals and medical ethics, whereby the law itself (the Human Fertilisation and Embryology Act 1990) was alleged to be in violation of Article 8.[506] In *Evans*, the legal accordance requirement was *intensely* scrutinised, with the ECtHR finding that the legal certainty afforded by the 1990 Act, and its provisions on consent, positively indicated the foreseeability and predictability of the law, consistent with Article 8's requirements.[507]

Intense scrutiny of this requirement is also observed where the State's discretion to act is considered too broad and not sufficiently precise. Such was the case in *LH v Latvia*

---

[502] *Malone v the United Kingdom* App no 8691/79 (ECtHR, 2 August 1984), para 67: 'there must be a measure of legal protection in domestic law against arbitrary interferences by public authorities'.
[503] *Silver and Others v the United Kingdom* (ECtHR, 25 March 1983), para 87: 'the law must be adequately accessible: the citizen must be able to have an indication that is adequate, in the circumstances, of the legal rules applicable to a given case'.
[504] *Sunday Times v The United Kingdom (*1979) Series A no 30, para 49. See McHarg (n 28) 685; van der Sloot (n 494) 4.
[505] McHarg (n 28) 685–686.
[506] *Evans v the United Kingdom* App no 6339/05 (ECtHR, 10 April 2007).
[507] ibid para 89.

where the ECtHR found imprecision in the law governing a Latvian public authority's ability to process the applicant's medical data – this was crucial to the reasoning of the decision and ultimately finding a violation of Article 8.[508] The legal remit of the public authority in question ('MADEKKI'[509]) was not clear in terms of what public interest it was carrying out in processing the applicant's personal data; the ECtHR thus found the applicable Latvian law without sufficient precision or protection against arbitrary interferences by the State.[510] The Court emphasised the fundamental importance of protecting an individual's personal (medical) data as 'It is crucial not only to respect the sense of privacy of a patient but also to preserve confidence in the medical profession and in the health services in general.'[511]

Therefore it seems where a public interest justification is used to process *sensitive* personal data (especially health data), the ECtHR will more intensely scrutinise the precision, foreseeability and the provision of safeguards in the law; the fact that data are kept safe and confidential is not likely to be enough.[512] Following the reasoning employed by the ECtHR in *LH v Latvia,* it would be critical to substantiate how data processing will specifically achieve the public interest aim relied upon (that data collected were potentially decisive, relevant or important to achieving that aim) – not dissimilar to considerations of the *necessity* of action.[513] As this is one of the few cases that involve both Article 8 and data protection issues, as well as specific consideration of the public interest, the approach taken in *LH v Latvia* is influential in sketching an overview of the requirement 'in accordance with the law' and its potential role in developing a new approach to determining what the public interest means in data protection.

---

[508] *Latvia* (n 493) paras 47-60.
[509] ibid. 'MADEKKI' being the public authority charged with monitoring the quality of medical care provision in Latvia.
[510] ibid paras 52, 59.
[511] ibid para 56.
[512] ibid para 58.
[513] ibid. Although the UKSC in *The Christian Institute* case held that as to a data sharing provision implicating a Scottish public authority, the use of data must not be merely objectively relevant but be 'significant' to the public interest aim sought. *The Christian Institute* (n 403) [56].

3.1.2.C 'Necessary in a democratic society'

Once the legitimacy and lawfulness of a Member State's actions are established, the ECtHR assesses the necessity of action. Within the context of Article 8, and the ECHR generally, necessity implies:

> [A] pressing social need; in particular, the measure employed must be proportionate to the legitimate aim pursued. In addition, the scope of the margin of appreciation enjoyed by the national authorities will depend not only on the nature of the aim of the restriction but also on the nature of the right involved.[514]

There are varying degrees of intensity with which the Court applies the 'necessary in a democratic society' test. As indicated previously, the ECtHR's interpretation of 'necessary' is of importance for the data protection context in the UK, as courts have adopted this approach when interpreting the DPA 1998.[515] The relative intensity applied to assessing the necessity of State action corresponds to the margin of appreciation afforded to States in a particular area such as security, economic welfare or morality. Generally, Member States are afforded a margin of appreciation to engage in 'the initial assessment of the reality of the pressing social need implied by the notion of "necessity" in this context.'[516] The ECtHR's assessment of 'necessity' is best illustrated by examining cases based upon different types of public interest justifications.

Security

A wide margin of appreciation is afforded to States in cases involving *national security* which can correspond to a laxer interpretation of necessity (as compared with cases involving other subject matter, such as economy security).[517] The wide margin of appreciation granted in matters of national security can be understood in the sense that individuals have no legitimate right to threaten a Member State's national security, such

---

[514] *Gillow* (n 386) para 55 as originally developed in *Handyside* (n 386) paras 48-49 (emphasis added).
[515] For example: *Daly* (n 85) [26]-[27]; *Ellis* (n 85) [1], [27]-[29]; *Stone* (n 85) [60]; *Corporate Officer* (n 85) [59]; *Catt* (n 85) [6]; *AB* (n 85).
[516] *Handyside* (n 386) para 48.
[517] For example: *Klass and Others versus Germany* App no 5029/71 (ECtHR, 6 September 1978); *Leander* (n 499) paras 59, 67; *Dalea v France* App no 58243/00 (ECtHR, 1 July 2008); *Kennedy v The United Kingdom* App no 26839/05 (ECtHR, 18 May 2010); *Uzun v Germany* App no 35623/05 (ECtHR, 2 September 2010). Similar analysis by van der Sloot (n 494) 13–14.

as through criminal activity. Where the crimes committed by an individual are particularly serious, the necessity of the State's interference plays a minimised role in the reasoning of the ECtHR decision, with more intense focus on the legality of action and proportionality; necessity is easier to justify where threats to the State and the public are more severe.[518] However, this wide margin of appreciation can be observed even in cases where the seriousness of the security threat posed is significantly less. In *Leander v Sweden* the Court accepted:

> that the margin of appreciation available to the respondent State in assessing the pressing social need in the present case, and in choosing the means for achieving the legitimate aim of protecting national security, was a wide one.[519]

The margin of appreciation was wide enough to justify the maintenance and use of a secret police-register to assess the applicant's suitability for employment in a position implicating apparent issues of national security; however it should be noted that his employment was for a temporary post in a museum merely adjacent to a secured naval base.[520] The decision in *Leander* suggests a level of deference to the Member State's own assessment of what is and is not a relatively 'important' threat to national security.

However, this supposed pattern of deference to matters of national security is called into question when in other cases the margin of appreciation appears to be narrowed, and necessity interpreted more strictly – even in light of what may be considered objectively 'serious' threats to national security, such as terrorism.[521] Stricter scrutiny of State claims to protect national security is also identified in cases where an unacceptable level of discretion is afforded to the State – here the focus is usually not on 'necessity' but the lack of precision in a Member State's law (and therefore whether the interference was 'in accordance with the law').[522] These observations suggest that even within a particular category of public interest justifications, such as 'national

---

[518] For example, in *Uzun v Germany* the applicants were alleged to have taken part in a series of bomb attacks. *Uzun* (n 517). Also: *Kennedy* (n 517).
[519] *Leander* (n 499) paras 59, 67.
[520] ibid paras 10, 21.
[521] For example: *Segerstedt-Wiberg and Others v. Sweden* App no 62332/00 (ECtHR, 6 June 2006); *Nada v Switzerland* App no 10593/08 (ECtHR, 12 September 2012).
[522] For example: *Rotaru v Romania* App no 28341/95 (ECtHR, 4 May 2000); *Liberty and Others v The United Kingdom* App no 58243/00 (ECtHR, 1 July 2008).

security', the ECtHR takes a very fact-sensitive and ad hoc approach to their decision-making. In the words of van der Sloot, the Court 'rather seems to use a rule of thumb' test for assessing necessity when it involves national security,[523] and thus the only pattern that can be deduced is the *lack* of any pattern at all.

Morality

The second category of 'public interest' cases examined involve issues of morality whereby a State's interference may impact upon extremely intimate aspects of individuals' lives, notably their sexuality.[524] Many historically prominent Article 8 cases involved the criminalisation of homosexual activity by Member State legislation.[525] In such cases, the ECtHR has adopted reasoning on the interpretation of 'necessity' from freedom of expression cases under Article 10 of the ECHR, which also involve issues of sexuality and morality.[526] When confronted with issues of sexuality, the ECtHR has shown a level of deference to Member States, affording a generally wide margin of appreciation because the 'requirements of morals varies from time to time and from place to place, especially in our era which is characterised by a rapid and far-reaching evolution of opinions on the subject.'[527] (There is an interesting parallel here with the contextual nature of the public interest concept and inability to 'pin it down' and predefine it in any particular context, a point to be considered in more depth in Section 4.) In this sense, States have been considered better placed to assess and act upon the moral sentiment of their society:

> By reason of their direct and continuous contact with the vital forces of their countries… [and] to give an opinion on the exact content of these requirements as well as on the 'necessity' of a 'restriction' or 'penalty' intended to meet them.[528]

---

[523] van der Sloot (n 494) 14.
[524] *Evans v the United Kingdom* (n 506) paras 59-60, 69; *SH and Others v Austria* App no 57813/00 (ECtHR 3 November 2011), paras 113-118.
[525] *Dudgeon v The United Kingdom* App no 7525/26 (ECtHR, 22 October 1981); *Norris v Ireland* Series A no 142 (ECtHR, 26 October 1988); *Modinos v Cyprus* Series A no 259 (ECtHR, 22 April 1993).
[526] From *Handyside* (n 386) para 48. But also: *Müller And Others v Switzerland* Series A no 133 (ECtHR, 24 May 1988) paras 31-37.
[527] *Handyside* (n 386) para 48.
[528] *Handyside* (n 386) para 48 (emphasis added). Similarly, *Evans v United Kingdom* (n 506) para 77.

Nevertheless the ECtHR has insisted upon their role in supervising this discretion afforded to Member States not least because of the potential impact upon the most intimate of areas in individuals' lives, such that 'there must exist particularly serious reasons before interferences on the part of the public authorities can be legitimate for the purposes of paragraph 2 of Article 8.'[529] In *Dudgeon v The United Kingdom*, while the ECtHR does acknowledge the generally wide margin of appreciation afforded to Member States in this area, the moral sentiment on homosexuality in Northern Ireland was *not* dispositive of a determination of necessity.[530] The ECtHR took specific account of the changing tide of European sentiment on homosexuality and generally increased tolerance,[531] which was critical to their finding of a violation of Article 8.

Ultimately, as with cases involving national security, no bright line rules can be formulated. While European consensus on a particular issue may at times result in stricter scrutiny of necessity (e.g. as in *Dudgeon*), in other cases (involving freedom of expression) the Court gives more weight to *local* sentiment despite wider (and potentially divergent) transnational/national views on a topic.[532] This inconsistent body of case law has invited criticisms of a 'missed opportunity' for the ECtHR to adopt a more robust standard of protection of rights.[533] The ad hoc approach taken may be an inherently 'flimsy' basis for protection of Article 8 as it applies to individuals' sexuality, but for present purposes the point is that this analysis underlines the unsystematic way the Court adjudicates rights versus public interests.[534]

The implications of the ECtHR approach for the concept of the public interest more generally indicates their contextually based understanding of the 'public' in the 'public interest', as distinct from ordinary usage which is associated with aggregate notions of the concept, including what is 'good for *everyone'* and 'good for *most*'.[535] The attention

---

[529] *Dudgeon* (n 525) para 52.
[530] ibid para 58.
[531] ibid para 60.
[532] These Article 10 cases are relevant as the ECtHR has adapted such reasoning into Article 8 decisions involving issues of morality. *Handyside* (n 386) paras 54-57; *Müller* (n 525) para 40.
[533] Steven Greer, 'The Exceptions to Articles 8 to 11 of the European Convention on Human Rights' (Council of Europe 1997) 25–29 <http://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-15(1997).pdf>; McHarg (n 28) 691.
[534] McHarg (n 28) 691.
[535] Mansbridge (n 49) 9.

paid to the multiplicity of 'publics' and stakeholders in making public interest determinations is indeed something to be regarded for developing a new understanding of the public interest concept in data protection.

Economic well-being

A similarly unsystematic approach is found in the ECtHR's evaluation of public interest justifications of an *economic* nature. Within this body of case law, the Court took an extremely narrow approach to the test of necessity, in the first string of cases to consider the issue. First, in *Funke v France*, the ECtHR indicated that the public interest 'exceptions' under Article 8(2) were to be interpreted *narrowly*. The Court required that a convincing case be established to justify the need for the interference in question, which in *Funke* was the 'need' to prevent capital outflows and tax evasion for the overall well-being of France's economy.[536] The Court's reasoning in *Funke*, and the related cases *Crémieux* and *Miailhe,* can be characterised by a 'priority to rights' approach, which results in stricter scrutiny of necessity. [537] These cases are in stark contrast to the much wider margin of appreciation given to State's economic interests in later cases such as *MS v Sweden*.[538]

In *MS v Sweden*, although the interference involved the applicant's sensitive personal data, data regarding previous abortions, the reasons for disclosure were considered relevant and sufficient to evaluating her application for compensation due to industrial injury (and thus necessary).[539] The stance taken in this case suggests a rather *low* threshold for States to justify action in pursuit of the economic well-being of a country, as opposed to the stricter standard imposed in cases such as *Funke*, *Crémieux* and *Miailhe*.

---

[536] *Funke* (n 501) para 55. This stricter line of reasoning was also adopted in the decisions of: *Crémieux v France* (1993) Series A no 256-B, para 38; *Miailhe v France* (1993) Series A no 256-C, para 36.
[537] Greer (n 533) 23.
[538] For example, *MS v Sweden* (ECtHR 27 August 1997), para 38; *Kennedy* (n 517) para 155. Van der Sloot contends that the ECtHR generally affords a wide margin of appreciation in cases involving economic well-being. van der Sloot (n 494) 16–17.
[539] *MS* (n 538) para 44.

This divergence in the interpretation of necessity merely reflects the similarly varied approach taken to the concept within the UK.[540] However, even if we are unable to extract clear patterns of a definitive standard for necessity from Article 8 jurisprudence, it clearly remains a crucial consideration where the rights of individuals are compromised. 'Necessary' is already consecrated within data protection law. The only way a data controller *can* lawfully process personal data, outside of obtaining an individual's consent, is if the processing is *necessary*. What is left unresolved, and cannot be determined from Article 8 jurisprudence, is precisely what standard of necessity is required if we are to deploy the concept in acknowledgement of *both* the public interest in protecting informational privacy *and* using personal data.

3.1.2.D Summary of the ECtHR approach to the public interest

Although the substantive meaning of the public interest in Article 8 is confined to the descriptive examples provided, the case law reveals crucial insights into the relationship between the public interest and 1) the relevant public(s) and 2) related procedural principles such as legality, necessity and proportionality. Even if the examination of Article 8 jurisprudence revealed an unsystematic approach to the public interest, the cases shed light on the reasonable range of circumstances where processing may be justified in the public interest.

From the analysis of cases involving issues of morality, the ECtHR demonstrated an understanding of the public, in the 'public interest', in a more dynamic way than conventional understandings of the term. In *Dudgeon*, the ECtHR displayed an understanding of the public interest which was beyond the mere majority interest, when it overrode the wide margin of appreciation afforded to Member States, the majority 'interest' in the UK that may be in favour of criminalising homosexuality, and ruled based on the wider, European sentiment and tolerance.[541] More generally, if we consider the Court's flexible (albeit unsystematic) approach to Article 8 cases, this reveals the extent to which the public interest, as a concept, must always be examined

---

[540] Ministry of Justice (n 417) 13; Black and Stevens (n 11) 103–108; ICO, 'When Is Processing Necessary?' <https://ico.org.uk/for-organisations/guide-to-data-protection/conditions-for-processing/>.
[541] *Dudgeon* (n 525) para 60.

in context. The Court's treatment of morality, reveals the importance of context when assessing the public interest: 'requirements of morals varies from time to time and from place to place, especially in our era which is characterised by a rapid and far-reaching evolution of opinions on the subject.'[542]

As to procedure, we can extract from Article 8 case law the importance of *legality*, *necessity* and *proportionality* when deciding matters involving conflicts between public and individual interests (and arguably conflicts with other public interests). While the case analysis above considered the ECtHR's specific interpretation of 'in accordance with the law' and 'necessity' in line with the requirements of Article 8, the principle of proportionality can be discerned from the seemingly ad hoc and disparate approach taken by the ECtHR to different Article 8 cases.

Consider McHarg's explanation of the disparity in the ECtHR's approach to interpreting necessity. According to McHarg, the Court decides Article 8 cases either according to a 'priority to rights' approach or a 'priority to the public interest' approach; and I would contend that this approach is guided by the underlying principle of *proportionality*. Under the former approach, the Court is primarily concerned with *the effect of the interference on a right*. In such cases the margin of appreciation is narrowed and the necessity test is more strictly applied.[543] In such cases the Court finds the intrusion upon the individual greater than the public interest aim served and therefore the Member State's actions are disproportionate (and not necessary). Under the latter approach, the ECtHR is more concerned with the *implications for the exception (the public interest being carried out)*. Here a more purposive analysis is undertaken as to the necessity of a State's interference and a wider margin of appreciation is afforded.[544] Again, I would argue that proportionality ultimately guides this difference in approach – the intrusion upon the individual in such cases may be considered slight or at least proportionate and necessary to the achievement of the public interest aim in question.

---

[542] *Handyside* (n 386) para 48.
[543] McHarg (n 28) 688. Seen in cases *Dudgeon* (n 525); *Funke* (n 501); *Rotaru* (n 522); *Liberty* (n 522).
[544] Seen in cases *Leander* (n 499)*; Klass* (n 517); *Handyside* (n 386); *Müller* (n 525).

Proportionality has its own distinct meaning in the context of the ECHR and Article 8 jurisprudence and I acknowledge that there are also differences in how the ECtHR interprets proportionality.[545] Rather, my point is that proportionality is an underlying principle which guides both the application of 'in accordance with the law' and 'necessity' and goes some way in explaining why such variance in approach is required, aside from the obvious contextual nature of such determinations.

However, we must return to the key question – what can Article 8 jurisprudence offer to developing a new understanding of the public interest concept in data protection? Principles for guiding procedure? Yes. But the Court's haphazard consideration of 'in accordance with the law' and 'necessary in a democratic society' is not sufficiently precise or predictable. While their approach to balancing individual privacy and the public interest is rightly context sensitive, recognising the dangers in 'fixing' any definition of the public interest, there have indeed been missed opportunities to provide more standardised guidance on how to deploy concepts such as necessity and legality where there *is* European consensus on a given issue. Furthermore, the procedural understanding and evaluation of the public interest under Article 8 is fundamentally flawed for the purposes of data protection because these assessments are made on the basis that protecting privacy serves only *private*, *individual* interests, and does not implicate broader, public interests. This requires a *balance* to be struck between protecting individual privacy on the one hand and the public interest on the other, which (wrongly) pegs the two against each other in a zero-sum game of opposition.[546]

In data protection, to consider the protection of privacy and the 'public interest' as poles apart, will always place the individual's interest at a disadvantage unless the harm caused to the individual can somehow be shown as carrying at least the same weight as the counter public interest at stake.[547] The risk is that this 'balancing' will, 'often [produce] unconvincing results that serve mainly the interests of whoever does the

[545] McHarg (n 28) 686–688.
[546] See Chapter 2 Section 3.2.3. Raab (n 168) 1.
[547] Black and Stevens (n 11); van der Sloot (n 494).

balancing: typically, those who value privacy less than other desirable qualities'.[548] A crucial component to developing a new understanding of the public interest in data protection is to first and foremost acknowledge the broader public interests, not only the private interests, served by protecting an individual's informational privacy. In this sense, this is where the approach to privacy and the public interest taken in regards to Article 8 diverges from what is being developed here for data protection. While Article 8 jurisprudence aids our understanding of procedure and the meaning of certain key concepts within the public interest conditions, we remain without a sense of the fuller, substantive meaning of the public interest in data protection or a means to normatively evaluate when the processing of personal data is justified in the public interest.

3.1.3 Deficient understandings of the public interest in the law

The analysis above, in combination with the previous chapters' examination of data protection law, illustrated the lack of a *substantive* understanding of the public interest in either the data protection or human rights context. The DPD, DPA 1998 and Article 8(2) merely provide an arbitrary and descriptive list of 'public interests'. These examples are provided without any criteria that can be used to explain what characterises a type of processing[549] as 'in the public interest' and others not.

Article 8 jurisprudence tells us that public interest determinations are context sensitive and that the public interest is not always equivalent to what is in the interests of the majority; the public interest may lie in the protection of a deeply important but minority held interest. This body of case law also reveals important insight into the role of procedural principles (legality, necessity, and proportionality) in deciding on matters of conflict between public and individual interests. While the UK courts have already adopted this approach for interpreting key aspects of the public interest conditions in the DPA 1998, it remains that we lack a substantive understanding of what the public interest means if a given form of processing does not fall within the list of examples provided. Assessing whether processing is in the public interest is a separate determination to addressing whether processing is lawful, necessary and proportionate.

---

[548] Raab (n 168). Also: Solove (n 197) ch 4; Ronald Dworkin, *Taking Rights Seriously* (Bloomsbury Publishing 2013) 239–241.
[549] Or Member State 'action' in context with Article 8(2) of the ECHR.

On this basis, we are left with the unacceptable prospect of future litigation to 'test' each case of data processing, and each unique set of facts, based on the public interest conditions. What role is there for drawing upon legal and political theory to inform a new conceptual understanding of the public interest in data protection?

4. Consulting Theory to Understand the Public Interest as a Concept in Data Protection Law

In this section I will draw upon legal and political theories of the public interest to address the conceptual inadequacies identified in the legal framework. Political and legal theory reveal the boundaries of the public interest as a concept, which can further our substantive understanding from the limited basis offered from the previous legal analysis. Although the public interest concept is similarly imbued with an element of uncertainty within these disciplines[550], the public interest nevertheless maintains an important space – in political science, philosophy and theory in particular – as demonstrated by the robust history of dialogue and analysis devoted to the concept.[551] This contrasts with the less frequent engagement with the substantive meaning of the concept in data protection. Furthermore, the methods used in these disciplines are not subject to the same constraints as the 'Rule of Law',[552] and thus alternative approaches are found for determining the substantive content of the public interest in a 'legitimate' way – legitimate in the sense that where the concept is used, supporting theory and explanations are indicative of *more than* mere compliance with the law; it indicates justification in a normative sense. I use these theories to interrogate the public interest conditions in data protection law and later use these explanations to derive criteria for assessing the public interest in each case.

---

[550] Sorauf (n 56) 617; Glendon A Schubert, *The Public Interest: A Critique of the Theory of a Political Concept* (The Free Press 1960) 223–224; Robert Dahl and Robert Lindblom, *Politics, Economics and Welfare* (Second, Transaction Publishers 2000) 503–504.

[551] 'No deliberation of politics and political theory claims a more venerable heritage than the dialogues on the existence, nature, and requirements of the "public interest" or the "common good"'. Bozeman (n 59) 15. Both Held and Bozeman provide valuable literature reviews on the study of the public interest in political science, theory and philosophy: Held, *The Public Interest and Individual Interests* (n 58) 203–228; Bozeman (n 59) 187–220.

[552] As understood in terms of Fuller's internal morality of the law, while recognising the competing conceptualisations of 'Rule of Law' not least including those proposed by Friedrich von Hayek, Albert Dicey and John Rawls. Fuller (n 474) 39.

In exploring theories of the public interest, a body of authoritative texts emerge. Through the lens of political philosopher Virginia Held's typology of the public interest, the dominant theories on the concept can be set forth within an accessible framework for the present analysis.[553] The relative strengths and weaknesses of each theory will be assessed for its capability to explain the 'logic' for including certain public interests explicitly in the law, and whether it can provide criteria to assess the public interest in processing more generally (especially where processing is unrelated to the examples specifically provided in the law). To be clear, my end goal is not to define a fixed concept. As indicated in the context of Article 8 jurisprudence, the public interest must always be examined *in context* and this limits the extent to which it can be defined in advance. It is only by examining and better understanding the various rival conceptions of the public interest that we can approximate the legitimate boundaries of the concept in data protection law, and ensure its use is confined to only appropriate circumstances.

4.1 A typology of the public interest

The starting point for our analysis begins with Held's typology of the public interest, where she classifies three main theories, the proponents of which each claim to provide the 'true' definition and understanding of the concept. These are:

> **Preponderance theories:**
> The public interest is equivalent to the majority of individual interests. It is equivalent to what provides the most pleasure and least pain to individuals. Although individuals and groups may have valid, conflicting interests, the public interest always lies with the preponderance of individual interests.[554]
>
> **Common interest theories:**
> The public interest is an interest that *all* members of the relevant public have in common. Individuals may have other justifiable interests, which conflict

[553] Held is widely recognised for her contribution to the study of the public interest. McHarg (n 28); Kadri Simm, 'The Concepts of Common Good and Public Interest: From Plato to Biobanking' (2011) 20 Cambridge Quarterly of Healthcare Ethics 554; van der Sloot (n 494).While there are critiques offered by Held's peers, as to her 1) methodology in developing the classification scheme and 2) own theory of the public interest and its relation to individual interests, Held's typology remains valuable to the study of the concept. For peer review of Held's analysis: Barry M Mitnick, 'A Typology of Conceptions of the Public Interest' (1976) 8 Administration & Society 5. David Braybrooke, 'Review: The Public Interest and Individual Interests. Virginia Held.' (1972) 69 The Journal of Philosophy 192.
[554] Held, *The Public Interest and Individual Interests* (n 58) 42–43, 49–98.

with this common interest, but the public interest serves such individuals as well; if not in the present, in the long run.[555]

Unitary theories of the public interest:
What is in the public interest for the community as a whole, is in the interest of the individual. Therefore, if 'x' is in the public interest, it cannot also be true that 'x' is not in the interest of any individual. If individuals interests conflict, their interests are invalid, given that the public interest is singular in nature and overrides any such conflict. [556]

Below, each of these theories will be assessed in terms of its ability to:

- explain and define the logic behind the existing 'list' of public interests provided in data protection law;
- identify public interests which do not fall explicitly within the text of existing law; and
- provide a legitimate procedure for deciding conflicts between two public interests, namely the public interest in protecting informational privacy and in certain uses of personal data.

4.1.1 Preponderance theories

Preponderance theories are most closely associated with aggregative and utilitarian conceptions of the public interest which equate the concept with the *majority* interest – the public interest lies with the course of action which delivers the most pleasure and least pain. Preponderance theories therefore include the work of Hobbes (the public interest arises once a preponderance of individuals' interests are best served by that interest)[557], Hume (the public interest lies in that which has utility for a preponderance of individuals)[558] and Bentham (there is no public; the public interest is merely the sum of the interests of its individual members)[559]. In a cruder but effective illustration, Sorauf equates preponderance theories with an exercise in counting noses,[560] meaning that this conception of the public interest does nothing more than indicate what the majority opinion is. This theory therefore translates to a form of utilitarianism whereby 'the public interest is equivalent to the greatest good for the greatest number'.[561]

---

[555] ibid 44–45, 99–134.
[556] ibid 45–46, 135–162.
[557] Hobbes (n 53).
[558] Hume (n 54).
[559] Bentham (n 55).
[560] Sorauf (n 56) 625.
[561] Bozeman (n 59) 209.

Applying the preponderance theory to the context of data protection would mean that the categories of public interests provided under the DPD and DPA 1998 were included because a preponderance of individuals believed (or were thought by decision-makers to have believed) that 'x' processing was in their interest. From the examination of the *travaux* to the DPD, we know this not to be true. The types of public interest processing enumerated under the DPD were included based on political negotiation between representatives of Member States, not because majority consensus was found for that type of processing. Where lobbying efforts were made, such as in the case of research,[562] it was not in response to an objective finding or a claim that such processing was in the interest of a preponderance of individuals. While it could be argued that by a population's election of their Member State's European Parliament representatives, that majority's opinions are expressed through these elected representatives and thus through their lobbying efforts during the drafting process, a preponderance theory remains at least an incomplete explanation, given the other political factors at work in negotiating and finalising a directive.[563]

If we accept that the types of processing designated as public interest examples in data protection law are *not* best understood through preponderance theories, what can these theories offer for determining whether *other* types of processing are justified in the public interest? It is entirely foreseeable that the views of a 'preponderance of individuals' might be offered as evidence, by a data controller, of the public interest in processing. However, to say that 'x' is in the interests of a preponderance of individuals means *only that* 'x' is one type of reason why we might find that it is also in the public interest[1] and *does not mean that* 'x' is necessarily and *normatively* in (or therefore justified by) the public interest.

---

562 From the DPD's *travaux*: 'Note from the UK Delegation to the Health Working Group: Implications for Health Research' (21 September 1994) 9415/94 3-5; 'Note from Denmark: 'Research related issues' (12 October 1994) 10934/94, 2-4.

563 Which involves the Council of the European Union and European Commission; only the views of European Parliament could be said to (potentially) implicate the majority opinion of its constituents in each Member State. 'EU Institutions and Other Bodies' <http://europa.eu/about-eu/institutions-bodies/>. Equally, the same reasoning could be rejected as to the public interest examples in the UK, per the DPPSPD 2000.

Under this theory 'x' is merely an empirical fact and does not provide a method to determine whether 'x' is in the public interest in a *normative* sense. If we are to determine whether a given 'x' is normatively in the public interest, Held asserts that:

> we want to know something *else* than the empirical fact that it is in the interests of a preponderance of individuals, although being in the interests of a preponderance of individuals may well be among the possible good reasons for believing that such an x is in the public interest.[564]

There are situations where majority opinion *is* dispositive on an issue, such as in the election of political representatives. However, the public interest is logically and necessarily distinct from what can be verified through empirical fact. The critical point being made here is that although the majority interest is *one* such factor that can be considered important to determining where the public interest lies, it cannot derive any *normative* value on its own – empirical facts do not answer *why* 'x' is or is not in the public interest.[565]

Preponderance theories are also unsuitable for application to the data protection context because such theories always favour the majority interest in situations of conflict, regardless of good contextual reasons to the contrary. To unpack this, let us first clarify what is meant by a 'preponderance of interest'. According to Held's taxonomy, preponderance theories describe the public interest by reference to '…a magnitude of some kind, either a degree of force, or a greater amount of sentiment, or a stronger level of opinion, or a numerical quantity of utility, or simply, a "higher" number.'[566] By reference to an extreme but illustrative example let us consider preponderance in terms of a numerical majority: If 'x' research use of data benefits only 49.5% of the public in question, this would not be in the public interest, while 'y' research use of data that benefits 50.5% would. This, one could argue, is prima facie absurd and cannot account for any normative difference in this 1% when the *qualitative* difference might be a matter of life or death for the individuals involved. (This is notwithstanding the undoubtedly countless issues that one would face if attempting to

[564] Held, *The Public Interest and Individual Interests* (n 58) 84.
[565] As also argued by: ibid.
[566] ibid 49.

derive the appropriate methodology to aggregate all the relevant set of individual preferences on an issue.)

To answer *why* this interpretation of the public interest (as the majority) is unsuitable for the data protection context we must consider the wider socio-legal context in which data protection law operates. Julius Cohen considered the relationship between the meaning of the public interest to a community and that community's basic values (as an element of the wider socio-legal context in which the public interest concept derives its meaning).[567] Cohen illustrates this by considering how the denial of something to a *minority* group, while in the interests and/or favoured by the *majority*, can nevertheless be counter to that community's values and thus interpretation of the public interest:

> To suggest, for example, that the public interest would not be involved if the Jehovah's Witnesses were denied freedom of expression by a statute supported by a majority of the population would fly seriously in the face of experience. For our community values include not only concern for the majority, but under certain circumstances, for the minority as well. Our values have a qualitative as well as a quantitative dimension. To put it another way, there is a public interest in the private rights of those who elect not to follow the crowd, *because it is consistent with one of our basic community values*.[568]

Applied to the UK and EU context, relevant community values for data processing decisions include those enshrined by human rights law, which in its broadest sense can be understood to protect individuals against tyranny by minority groups (dictatorships), tyranny by the majority, or mob rule, by giving individuals rights against the collective.[569] For the public interest conditions to processing to have any internal consistency with the other data protection principles (e.g. fairness, data minimisation and so forth), or external coherence with human rights legislation, intrusions by the collective into the sphere of the individual (via data processing) cannot be defensible merely because the numbers weigh more heavily in favour of the 'public' which a

---

[567] I use the term 'values' in its most basic and traditional sense; and although a discussion on 'values' as a concept is beyond the scope of this thesis, it is pertinent to note Cohen's interpretation which I would adopt for this discussion: 'They are values held by humans; they concern the relational aspects of man in his social capacity; they are shared by humans, and in this sense take on the aspect of common or community values.' Julius Cohen, 'A Lawman's View of the Public Interest' in Carl J Friedrich (ed), *Nomos V: The Public Interest* (Atherton Press 1962) 157.
[568] ibid.
[569] Ronald Dworkin, *Taking Rights Seriously* (Bloomsbury Academic 2013) 116–119, 432.

preponderance theory of the concept would allow. This would be prima facie *inconsistent* with the purpose and values enshrined by both data protection and the overarching system of human rights law in the EU. What is needed is not mere head counting, but an understanding of the public interest that is both quantitatively *and* qualitatively informed.

Even if only a small number of individuals would benefit from a processing initiative, it may still be justifiable 'in the public interest'. For example, certain types of scientific research, such as that involving rare diseases, will only ever directly benefit a specific and small portion of the public, not a 'preponderance' of individuals if understood as a crude majority. It is arguable that such research still embodies what the public interest concept means, if quantitative factors are not treated as dispositive on the issue. Additionally, a further reason to reject preponderance theories *not* based on an intuitive appeal to fairness to the vital interest of a minority, is a Rawlsian argument of enlightened self-interest. According to his view, a distribution of goods (and also risks) is fair if we would choose it under a condition of ignorance – that is without knowing if we would personally benefit.[570] Even this type of second order reasoning about 'fair preferences' remains precluded by the type of preponderance theory discussed here.

Considering the public interest through the lens of deliberative democracy, Ian Flynn provides that 'deliberative democracy is well placed not just to deliver the public interest, but also to identify those exceptional cases where a special interest justifiably overrides a public interest.'[571] While I am not arguing that informational privacy is a 'special interest', distinct from the 'public interest', it is important that any theory of public interest is capable of identifying cases where the public interest in protecting informational privacy must *outweigh* the public interest benefits of processing, even if the majority opinion sides with the latter. Interpreting the public interest conditions to processing according to a preponderance theory would perpetually place the protection of informational privacy at a disadvantage when weighed against the public interest as representative of a majority that may benefit from a form of data processing. Such

[570] John Rawls, *A Theory of Justice* (Harvard University Press 2009) 11, 75, 118.
[571] O'Flynn (n 49) 311.

theories cannot account for important nuances, such as the intensity with which an interest is held, even if by a minority of individuals – again speaking to the inability to derive any normative understanding of the concept. Any theory which equates the public interest with calculations '…for the aggregation or maximization of interest satisfaction are inherently incapable of taking adequate account of consideration of justice and of rights'[572] which data protection law must capable of doing to remain consistent with its own principles and with external community values such as those enshrined by human rights legislation.

A new understanding of the public interest in data protection must indeed account for the interests of 'publics' and whether the preponderance of individuals is for, or against, particular uses or methods of using data. There is a need for significantly more public dialogue over the constantly evolving uses of personal data by both private and public actors. However, empirical facts are not in themselves dispositive of what is or is not in the public interest in a normative sense even if increased public dialogue on an issue is an important part of the process for determining how a decision based on the public interest should be taken.[573] The interests of individuals as to any data initiative may represent one aspect or vision of the public interest, which should be considered as part of the resolution of the relevant spectrum of public (and private) interests at stake. A different theory is required to explain and decide on matters of the public interest in data protection law even if the preponderance of individuals' interests is one component to consider.

4.1.2 Common interest theories

Following Held's typology, the second theory includes common interest theories which reason that the public interest lies where interests are unanimously held, '…interests which all members of a community have in common.'[574] Common interest theories include Rousseau's conception of the public interest. This refers to Rousseau's idea of

[572] Held, *Rights and Goods: Justifying Social Action* (n 58) 144.
[573] Richard E Flathman, '34. The Public Interest: Descriptive Meaning', *Concepts in Social and Political Philosophy* (Macmillan Publishing Co, Inc 1973) 531; Bozeman (n 59) 226–235 citing John Dewey, The public and its problems (1927).
[574] Held, *The Public Interest and Individual Interests* (n 58) 99.

'the general will' derived from all the 'pluses' and 'minuses' of individual wills which when balanced always give way to the common interest.[575] A contemporary account of common interest theory is found in Bart van der Sloot's analysis of Article 8 jurisprudence. [576] Van der Sloot characterises the ECtHR's approach to the public interest as a 'common interest' approach whereby interferences by a Member State are justified on the basis that they are ultimately in the interest of all members of a society.[577] Similarly, Aileen McHarg considers that the 'list' of public interests provided in Article 8 are 'pure public interests' given their 'exclusively collective nature' or that they 'benefit the public generally as well as identifiable individuals.' [578]

A well-known account of common interest theory is Brian Barry's in *Political Argument* (1965), where he defines the public interest as 'equivalent to "those interests which people have in common *qua* members of the public."' [579] Barry understands the meaning of 'public', for the purposes of determining the common interest, as decisively context sensitive:

> Instead of speaking in blanket terms about people or groups with common or opposed interests, we should speak of people or groups whose interests coincide or conflict with respect to the adoption of x rather than y.[580]

For Barry, 'We cannot therefore speak of what "the public interest" requires until we know the particular context in which the question is being raised.'[581] A context sensitive approach to understanding the 'public' in the public interest is seemingly taken at times by the ECtHR, identifying the relevant public more or less broadly depending upon the facts of a case.[582] For Barry, a starting point for determining the common interest would be to determine which people, groups or public is involved in the adoption of a particular course of action; who supports 'x' rather than 'y'?

---

[575] Jean-Jacques Rousseau, *On The Social Contract* (Drew Silver ed, GDH Cole tr, Dover Publications, Inc 2003) 17–18.
[576] van der Sloot (n 494) 24.
[577] ibid.
[578] McHarg (n 28).
[579] Barry (n 57) 190 (emphasis added).
[580] ibid 196.
[581] ibid 192 (emphasis added).
[582] *Handyside* (n 386) paras 54-57; *Müller* (n 525) para 40.

As to the commonality requirement of this theory, Barry concedes the impossibility of 'true' unanimity on any given interest,[583] and 'overcomes' this by suggesting (along similar lines to Rousseau) the idea of common *net* interests. Common net interests are determined by reference to how an individual is affected overall, striking a balance between the pluses and minuses incurred in his various capacities.[584] Barry (as did Rousseau) focuses on the different roles individuals play in society and that in accordance with those different capacities, their interests might diverge from the 'common interest'. However, 'One of the roles in which everyone sometimes finds himself or herself is that of "a member of the public."'[585]

When individuals identify themselves in the role of a 'member of the public', they 'will naturally tend to favour goods or policies that are in the interest of everyone in society, rather than goods or policies that benefit us in some more particular role.'[586] Thus for both Barry and Rousseau, any conflict between *individual* interests, which are specific to a particular role or capacity individuals play in society, is logically distinct from an individual's 'net interest' in a policy which relates to their role as a member of the public. Despite any conflict that may arise on an 'individual' (specific role/capacity) level, conflict is disintegrated when appropriate balancing is undertaken and an individual's 'net' interest as a member of the public is revealed. However, absent true unanimity, it is arguable that common interest theories come dangerously close to preponderance theories. The difference here is that individuals are *idealised* – the focus is not on the preponderance of individuals' views or preferences on a matter, rather, it is about what individuals *should* want if they understood fully the long-term benefits and disadvantages.[587]

Pareto's criterion of optimality for economic changes corresponds with the rationale of 'net common interest', whereby the public interest is understood in terms of changes where at least one individual in a group is made better off (in terms of their utility

---

[583] Barry (n 57) 195–196.
[584] ibid 196.
[585] O'Flynn (n 49) 305.
[586] ibid.
[587] Which might be considered as 'paternalistic preponderance theory', a point made originally by my supervisor, Professor Burkhard Schafer.

values) without anyone being made worse off.[588] James Buchanan and Gordon Tullock adopt a similar theory in *The Calculus of Consent* (1962) which discerns 'better' from 'worse' changes, and thus the public interest, on the basis of a unanimous decision by all members of a group.[589] However, for Buchanan and Tullock, 'The "public interest" becomes meaningful only in terms of the operation of the rules for decision-making'[590] and therefore their work focuses on the *procedure* involved in determining the common interest.

In a contemporary account of the public interest, providing one of the few analyses on the concept within data protection, Mark Taylor considers the public interest in the research use of genetic data.[591] Taylor focuses on the role of the public interest in decision-making:

> if you tie the idea of the public interest to the idea of common interests, then the legitimacy of public interest decision-making is dependent upon the ability of the system to account for common interests within the decision-making processes.[592]

Taylor considers whether the common interest may be the most plausible of theories on the concept,[593] however he does not ultimately favour any single theory, except to say that *legitimate* public interest decision-making must be able to transparently and justifiably account for the displacement of one interest over another (i.e. displacing an individual interest for a common interest or vice versa).[594]

The importance of procedure to determining the public interest finds synergies with theories on deliberative democracy. These are important to consider, albeit briefly, to acknowledge theories which equate the procedural legitimacy of deliberative democracy as a decision-making tool and the public interest as one in the same:

---

588 Held, *The Public Interest and Individual Interests* (n 58) 107–108. Per Vilfredo Pareto, *Cours d'Economie Politique (Lausanne, 1897)* II, 90ff.
589 James M Buchanan and Gordon Tullock, *The Calculus of Consent: Logical Foundations of Constitutional Democracy* (Library of Economics and Liberty 1999).
590 ibid 285.
591 Taylor (n 28).
592 ibid 30.
593 ibid 29.
594 ibid 31.

> [individual interests] can be filtered and transformed through a well-designed deliberative process so that the decisions that emerge will be in the public interest. On this pluralist view, therefore, deliberative democracy is treated as definitive of the public interest - i.e., the public interest cannot be determined until deliberation concludes and a decision has been reached.[595]

Unlike this procedural view on the public interest, others within this field find that the public interest remains identifiable and separate from related decision-making procedures.[596] Any new approach to understanding the public interest concept in data protection must offer substance and not merely more procedure. A new approach must indeed be capable of legitimately determining what processing is justifiable in the public interest when considering conflicts with the public and private interests in protecting informational privacy. However, a level of justification is needed beyond mere (substantiation of) compliance with legal procedure. The conceptualisation of the public interest being developed in this thesis certainly treats a claim that a certain form processing is in the 'public interest' as being indicative of something *more* than mere compliance with a given decision-making procedure. The entire reason for exploring theories on the public interest is to provide a deeper understanding of the public interest *concept* and thus the appropriate limits within which it can be relied upon by data controllers. By offering a clearer account of what may or may not be considered in the public interest, in a *substantive* sense, procedures can be designed in a way that is true to an agreed understanding of the concept. This could better account for the full range of interests and would be developed to avoid the conceptual vulnerabilities highlighted by Mansbridge's work on the essential contestability of the public interest.[597]

When applied to the data protection context it would therefore seem that common interest theories, both historical and contemporary, fall short of providing a

---

[595] O'Flynn (n 49) 302. In reference to Seyla Benhabib's approach to deliberative democracy: Seyla Benhabib, 'Toward a Deliberative Model of Democratic Legitimacy' in Seyla Benhabib (ed), *Democracy and difference: Contesting the boundaries of the political* (PUP 1996) 73.

[596] It is beyond the scope of this thesis to engage more fully in the area of deliberative democracy; it is merely used here to indicate the presence of theories which equate procedural legitimacy with the public interest i.e. if the decision-making procedure is legitimate, the result of that procedure will be 'in the public interest'. O'Flynn (n 49).

[597] Mansbridge (n 49).

comprehensive explanation for the meaning of the public interest. First, the key feature of common interest theories, the idea of unanimity or 'net' unanimity, is inherently problematic as it implies the existence of a public (common) interest over and above any conflicting individual interests.[598] The current 'list' of public interests are not provided in data protection law on the basis that any given interest, such as in research, would *always* be in the interest of all individuals and was commonly accepted as such – not even 'in the long run'. Rather, it is the nature of law to deal with conflicts and to offer a framework for making decisions in particular cases.

The legal framework in data protection recognises that for any use of personal data, an individual's interests and rights to informational privacy are at stake, but as I suggest, this should also recognise the *public interests* in the protection of informational privacy among any other interests which run counter to the use of personal data. The inherent conflict between the protection and use of data is recognised in cases involving Article 8 where the mere collection or disclosure of personal data can constitute an interference with an individual's privacy.[599] The list of public interests provided under the law are examples of processing which *may* justifiably interfere with an individual's informational privacy – they do not represent a unanimous consensus on the matter, or declare in any final sense, that a particular type of processing will always be justifiable in the public interest. Hence the procedural requirements under both data protection law and Article 8, for lawfulness, necessity, and proportionality.

A second ground for rejecting common interest theories is that they wrongly reduce considerations of the public interest to individual interests. The common interest is derived from the interests of individuals. What makes them 'public' is the extent to which they are 'common' amongst those individuals. Common interest theorists would ask: What would be good for individuals in that public? As opposed to: What would be good for the public, to which a group of individuals belong? This denies any aspect of the public interest which may be comprised of functions different from the function of its component parts i.e. individuals.[600] Motivations other than self-interest are thus

[598] Held, *The Public Interest and Individual Interests* (n 58) 99.
[599] *MS* (n 538) para 35; *Latvia* (n 493) para 33.
[600] Mansbridge (n 49) 10.

excluded from explaining what may be considered as 'in the common interest'. An individual's support of the 'common interest' is always explained in terms of their potential gain (no matter how unlikely).

One strategy to give additional reasons against common interest theories has drawn on the prisoner's dilemma.[601] Held uses this scenario to argue that 'One cannot justify socially cooperative behavior – or mutual trust – solely in terms of individual interest.'[602]

> If *both* [prisoners] choose the riskier course of not confessing, both will be better off than if both choose the purely self-interested course of confessing. But any justification for doing so must be based on something *else than* individual interest.[603]

Thus, Held is making the argument that as an empirical fact, we may have motivations that conflict with the prisoner's dilemma. Admittedly, Held's use of the prisoner's dilemma diverges from other analyses, notably David Gauthier's.[604] Gauthier's account of the prisoner's dilemma is premised on the idea that individuals have rational and *self-interested* reasons for acting in a cooperative manner, that in fact 'The moral man is no less concerned with his own well-being than is the prudent man, but he recognizes that an exclusive attention to that well-being would prevent him from participation in mutually beneficial agreements.'[605] Even if we accept that there are rational and self-interested reasons why an individual might choose cooperative courses of action, the conditions required by the prisoner's dilemma (notably the lack of communication and lack of enforcement) mean that it cannot be directly applied to the context under consideration here as decisions on the processing of personal data occur within an environment where dialogue and relevant enforcement *is* in place.

---

601 Originally devised by Merrill Flood and Melvin Dresher in 1950 as part of the Rand Corporation's research into game theory; however, the name 'prisoner's dilemma' was given by Albert Tucker when delivering a talk at Stanford University in 1950. Tucker A. W. (1950) A two-person dilemma (unpublished notes)
602 Held, *The Public Interest and Individual Interests* (n 58) 129.
603 ibid 128 (original emphasis).
604 David Gauthier, 'Reason and Maximization' (1975) 4 Canadian Journal of Philosophy 411, 425 <http://dx.doi.org/10.1080/00455091.1975.10716949>.
605 ibid 432.

Moreover, common interest theories of the public interest remain inappropriate for the data protection context for the other compelling reasons already set forth above. Most crucially, the public interest concept in data protection cannot be reduced to or resolved by a decisive common interest. Even if 'x' data processing has been previously understood as being in the public interest that does not imply that 'x' will always be in the public interest in a final sense and therefore always give reason to override the public (and private) interest in protecting informational privacy. Any understanding of the public interest, however commonly accepted, must be routinely scrutinised within the context at hand, which is something common interest theories would not provide for once the apparent unanimity in the relevant public interest is established.

As such, a more valuable conception of the public interest would be able to 'apply to a situation of conflicting, rather than common, individual interests' which is not possible based on the unanimous (or even 'net' unanimous) quality of common interest theories.[606] Data protection law exists *in light of* the inevitability of conflict between the protection of informational privacy and in the use of personal data.

In this sense, conflicts between multiple visions of the public interest are unavoidable and what we are reminded of from this analysis is that neither the public interest in protecting informational privacy nor in certain uses of data will be dispositive in all situations. Unanimity and the public interest do not go hand in hand.

4.1.3 Unitary theories

The final category in Held's typology are unitary theories, which focus on the normative quality of the public interest and centre around issues of morality.[607] Unitary theories are epitomised by Plato's theory on the common good, which provides that a greater good for society exists 'such that no member of it can have a genuine interest contrary to it.'[608] At the essence of unitary theories lies 'an overriding interest which

[606] Held, *The Public Interest and Individual Interests* (n 58) 127.
[607] ibid 135.
[608] ibid 139.

transcends and reconciles apparently conflicting individual or sectional interests.'[609] It can be said that unitary theories make no claim at being public: 'Its validity as the public interest depends not on the amount of acceptance it has, but on the superiority of its claim to rationality or wisdom.'[610] Therefore individual interests hold no relevance to this theory – how commonly held individuals hold an interest is irrelevant. Moreover, any individual interest which is contrary to the public interest is considered invalid under a unitary scheme of moral judgments.[611] The irrelevance of individual interests is what differentiates unitary theories from common interest theories. Individual motivations or interests simply do not factor into the calculation of the public interest (even if individuals would agree that 'x' is unitarily in the public interest); the public interest is beneficial for *everyone* even if individuals do not recognise it as such.[612] In other words, individual interests can never create imperatives concerning the public interest.[613]

Unitary theories offer something appealing to the approach being developed in this thesis: namely, that the public interest is not reduced to the mere counting of noses (in the words of Sorauf) and therefore may be able to explain *why* something is in the public interest beyond what can be explained in terms of offering direct benefit to any individual or segment of society. Unitary theories define the public interest by reference to an absolute system of values, which provide 'a unitary scheme of moral judgments which should guide every individual at a given time and place, although these individuals may be unaware of it.'[614]

A particularly good example of this would be religious value systems which aim to give guidance for correct behaviour in all aspects of life. However, for pluralist, secular societies, an equivalent system is difficult to envisage. It is true that in some countries, constitutions or human rights legislation may hold importance equivalent to the status

---

609 McHarg (n 28).
610 Sorauf (n 56) 626.
611 Held, *The Public Interest and Individual Interests* (n 58) 135.
612 CW Cassinelli, 'The Public Interest in Political Ethics', *Nomos V: The Public Interest* (Atherton Press 1962).
613 Richard E Flathman, *The Public Interest: An Essay Concerning the Normative Discourse of Politics* (John Wiley & Sons, Inc 1966).
614 Held, *The Public Interest and Individual Interests* (n 58) 135.

of religious doctrines that could potentially provide this system of values. Concepts such as 'constitutional patriotism' embody this idea.[615] Others may even try to add to the constitutional provisions some additional substance to the concept of a 'dominant culture' (*Leitkultur*) [616] which brings this 'constitution plus' model closer to Rousseau's notion of the general will. But even in these cases, at least in Europe and its liberal democracies, these socio-political artefacts hold their position of importance *because* they facilitate *different* conceptions of 'the good life' and thus different conceptions of the public interest to flourish.

Unitary theories are highly problematic for the context at hand given that it demands 'a *valid* judgment that a given measure, decision or arrangement is in the public interest rules out the possibility that conflicting individual claims of interest … may also be valid.'[617] In data protection law it is fundamental that conflicting claims of individual and public interests remain valid even where a particular decision may favour one or the other – the public interest in a particular form of data processing does not cancel out the public interest in protecting the individuals' privacy in question, nor does it call into question that the side that 'lost' are citizens of equal standing. As a result, unitary theories that are compatible with the vision of a liberal democracy will inevitably be too general and abstract to allow adjudication of conflicting public interests (note the plural) in a given case, while more substantive unitary conceptions inevitably are in conflict with the basic ideal of pluralist democracy of which data protection law is one expression.

In data protection (as in any other context) there is simply no 'philosopher-king' who knows in an absolute sense what the public interest is. Indeed, as just argued in the previous section, the approach and understanding being developed here singularly rejects the idea that the public interest is representative of anything in an absolute or final sense. The idea of a universal moral order that governs determination of all

---

615 Jan-Werner Müller, 'A General Theory of Constitutional Patriotism' (2008) 6 International Journal of Constitutional Law 72 <http://dx.doi.org/10.1093/icon/mom037>; Jürgen Habermas, *Between Facts and Norms: Contribution to a Discourse Theory of Law and Democracy* (MIT Press 1996) 491–515, 566–567.
616 'A Leitkultur for Germany - What Exactly Does It Mean?' (*(German) Federal Ministry of the Interior*, 2017) <http://www.bmi.bund.de/SharedDocs/Interviews/EN/2017/namensartikel-bild.html>.
617 Held, *The Public Interest and Individual Interests* (n 58) 135.

judgments (in a final sense), and thus distinguishes in a fixed black and white manner that which is on the side of goodness, and on the other badness, must be rejected. Such an approach is contrary to the fundamental aims of data protection law which recognises both the public interest in certain uses of data and in the protection of informational privacy. Just as a majoritarian approach (under preponderance theories) may lead to marginalisation of minority interests, unitary theories can also result in 'an increase of intolerance and righteous indignation' justifying disproportionate interferences with individuals' privacy in the name of national security for example.[618]

In the data protection context, the protection of informational privacy and certain uses of personal data must *both* be capable of being considered 'in the public interest' (the latter within restricted means i.e. in the UK, if considered 'necessary' and related to the function of a 'public nature'). No use of data will *always* be justifiable in the public interest, hence the importance of the procedural safeguards within data protection law. Equally, the protection of informational privacy is not absolute – the processing of personal data *can* proceed subject to a data controller's adherence to the relevant legal and procedural principles. Neither a proposed use of data nor the protection of informational privacy will always be on the side of 'good' or 'bad' in the sense demanded by unitary theories, which make all such conceptions unsuitable for the task at hand.

Finally, unitary theories of the public interest are most susceptible to misuse in data protection by those that would invoke them, and thus run counter to the understanding of the public interest being developed here which is to avoid the vulnerabilities of the concept highlighted in Section 2 above.[619] Any conception of the public interest in data protection must value individuals' interests (and society's interests) in informational privacy as *valid*, allowing for conflict with the public interests in certain uses of data. Furthermore, public interest determinations cannot be solely informed by the views of an 'authority' that claims to know the singular truth of what is or is not in the public

---

[618] ibid 155.

[619] 'The public interest as superior wisdom is often held by no larger a group than countless other interests in American politics…Their identification with the public interest reveals only brazen self-confidence and tactical shrewdness.' Sorauf (n 56) 626.

interest. As argued by Taylor, if decisions based on the public interest are to be *legitimate*, the decision-making processes must be transparent and justifiably account for the displacement of one interest over another (e.g. giving acceptable reasons for displacing an individual interest for a public interest). [620] When it comes to the public interest in data protection there are necessarily multiple interests, which will often result in conflict between valid claims of public and private interests that unitary theories cannot cater to.

4.1.4 Held's theory of the public interest

Although not directly attributed to any theory within her typology of the public interest, the main premise of Held's work was to consider how claims of the public interest relate to *individual* interests. Her intention was to:

> indicate the ways in which claims of public interest and individual interest may be related to each other, and to suggest that an adequate conception of the public interest should indicate that 'x is (is not) in the public interest' is a normative judgment, but that the validity of it should not imply or require the invalidity of the judgment 'x is not (is) in the interest of I', which may also be a normative judgment.[621]

It is through the lens and understanding of individual interests that Held develops an understanding of how the public interest interacts with conflicting individuals' interests. On this she proposes that individual interests may be understood as:

> 'X is in the interest of [the individual]' is equivalent to 'a claim by or in behalf of [the individual] for x is asserted as justifiable.'[622]

Held extends this reasoning to the concept of the public interest, similarly finding that the public interest may be understood as:

> 'X is in the public interest' is equivalent to 'a claim by or in behalf of the political system for x is asserted as justifiable.'[623]

---

[620] Taylor (n 28) 31.
[621] Held, *The Public Interest and Individual Interests* (n 58) 190.
[622] ibid 163–164 (emphasis added).
[623] ibid 167 (emphasis added).

This theory emphasises the *normativity* of both individual and public interests; to say something is or is not in the interest of an individual or the public, is to say something is *justifiable* – capable of being proven or demonstrated as 'just', 'right' or 'reasonable'[624].

Central to Held's theory is the idea that those with 'authority' make public interest claims on behalf of a political system because such claims are *justifiable.*[625] The requirement that a public interest claim be *justifiable* is what Held considers to be the normative element of the public interest. According to Held, 'Anyone asserting a public interest claim is asserting that a given action, decision, or policy *ought* to be effected or maintained by the polity; he is asserting that it is *justifiable*'.[626] This means, public interest determinations must be based upon reasons which would be acceptable to those whose rights are in the balance.[627] This relates to the need for legitimate procedures for determining the public interest while not conflating mere procedure with what is or is not in the public interest in a substantive and normative sense.

Held takes a practical approach to legitimacy, recognising that, 'In a political system, as in a legal one, decisions are and have to be made' and such decisions 'may appeal to a wide variety of justificatory considerations, some strong and reasonable, some weak and foolish.'[628] Decisions may be based upon the majority opinion of individuals, upon legal rules and reasoning, acceptable precedents, or a combination of these, but what is crucial to Held's theory is that 'a valid judgment that *x* is in the public interest does not … imply that judgments of individual interest in conflict with it are invalid.'[629] This raises a critical point for the context of data protection given that a claim that 'x' form of data processing is justifiable in the public interest does *not* invalidate the public interest and importance in protecting informational privacy. A decision procedure cannot claim to *resolve* the public interest in a final sense. Rather, an agreed procedure can only offer a decision to the extent that one is needed. The public (and private)

---

[624] Justify is defined in the Merriam-Webster Dictionary as 'to prove or show to be just, right, or reasonable'.
[625] Held, *The Public Interest and Individual Interests* (n 58) 184; Taylor (n 28) 30–32.
[626] Held, *The Public Interest and Individual Interests* (n 58) 185.
[627] Also as argued by Taylor. Taylor (n 65) 7–8; Taylor (n 28) 30–32.
[628] Held, *The Public Interest and Individual Interests* (n 58) 185.
[629] ibid 186.

interests at stake will continue as conflicting afterwards, which is consistent with an understanding of the public interest as an essentially contested concept that reflects the *multiplicity* of the public interest. A *legitimate* procedure for assessing the public interest in data processing must recognise the public interests in both protecting informational privacy and in certain uses of personal data.

While Held's focus is on the relationship between individual interests and public interests, she does consider the potential resolution of 'rival' claims of the public interest. In this regard, she suggests that 'any dispute between them can only be settled by going beyond the systems of both, even when a preponderance of individuals may give weight to one side or the other.[630] This would require 'A more inclusive system, containing both a political system and separate individual systems … in order to consider the relations between such rival claims.'[631] Held suggests appeals to ethical norms as an example. In later work, Held considers appealing to moral theories to resolve such conflict:

> we ought to appeal to moral theories that do connect with specific contexts, especially with some areas of applied ethics in which we have a grip on what some problems are and what some solutions to them might be like.[632]

Held is emphasising the important contextual element of assessing the public interest; that such decisions must be made from the perspective and context at issue. Held further contends that what is problematic for public interest determinations *in law* is that it necessarily involves political reasoning. Political reasoning requires *teleological* considerations whereas *deontological* justifications are characteristic of and appropriate to legal systems.[633] Whereas the law revolves around obligations and rights, the public interest concept raises issues that cannot be adequately resolved by reference to legal rules and principles.[634]

---

[630] ibid 188.
[631] ibid.
[632] Held, *Rights and Goods: Justifying Social Action* (n 58) 2–3.
[633] ibid 104–120.
[634] Held, 'Justification: Legal and Political' (n 58) 14.

There are no clear rules or a deontological basis for assessing the public interest in processing under data protection law, except to the extent that Article 8 and its procedural framework applies to a given case (in terms of assessing 'in accordance with law' and 'necessity'). The solution may lie in making '…a prior moral decision that a given procedure is appropriate for a given kind of issue', namely for determining when the processing of personal data is justifiable based on the public interest.[635] While no such decision has been made, a new approach could be devised that accounts for both the acceptable legal *and* conceptual parameters of the public interest. Such an approach could provide a more legitimate basis for assessing the public interest in processing – one that caters to the full range of public and private interests involved while remaining true to the legal, conceptual and normative dimensions of the concept. The chapter will conclude by briefly reviewing those features of public interest theory that can supplement the current and deficient legal understanding of the concept, which I later use to develop my own new approach to understanding the public interest in data protection.

5. Conclusion: Combining Law and Theory

The current state of data protection law is such that the public interest conditions are explained only in terms of descriptive examples and procedures (which are not even widely understood in practice). The public interest conditions require data controllers to independently determine in the first instance whether their processing of personal data is 'in the public interest' but there is no commonly accepted understanding of what the public interest means as applied to these conditions. The *travaux* in Chapter 3 revealed clearly that the public interests in the DPD were included for political reasons and were not subject to any assessment criteria to determine whether the processing was in the public interest in a substantive sense. Similarly, no criteria were provided in the UK's transposition of the DPD in the DPA 1998. This means that the current understandings of the public interest in data protection, which are based merely on examples and procedure, fall prey to the conceptual vulnerabilities highlighted in this chapter. In expanding the legal analysis in this chapter to Article 8 jurisprudence,

[635] ibid 15.

we learned more about the relationship between the public interest concept and the procedural principles of legality, necessity and proportionality. The ECtHR's approach to different public interest justifications in Article 8 cases emphasised the inherently contextual nature of the public interest. Nevertheless, we were left without any further direction on the substantive meaning of the public interest.

To fill the conceptual gaps identified from the foregoing legal analysis, political and legal theory of the public interest was examined. From preponderance theories, we can acknowledge that the public's views on any given form of data processing is an important element or even potentially one iteration of the public interest. However, we must also recognise the importance of *not* equating the public interest with the majority interest. This is to ensure that the 'individual' aspect of protecting privacy is not consistently overridden by apparent collective benefits to be reaped from a use of data (which ignores the broader, societal interests in protecting privacy).

Common interest theories helped to address the question of how 'public' a public interest must be. Of significance is Brian Barry's work which rightly identifies the first order of business in making public interest determinations – to find out 'which public' or 'publics' are implicated by a particular course of action. Also persuasive is Barry's recognition of the conflicting nature of individual interests and public interests because of the multiplicity of roles we each play in society. His theory on 'net common interests' can be used to overcome the impossibility of unanimity while recognising that there are certain 'interests' which are indeed public, but possibly only in a narrower and context sensitive sense.

Consideration of unitary theories revealed understandings of the public interest that appeal to a higher order of values, which determine in a final sense, what is or is not in the public interest. While unitary theories do not allow for multiple public interests to exist (and therefore are inappropriate for the purposes of data protection), they do offer an alternative explanation for defining the normative content of the concept without resorting to majority opinions or requiring unanimous consensus on a given matter. Such theories provide an explanation for the public interest beyond the individual, and thus beyond self-interest, which could be helpful in explaining the more

altruistic elements behind the public interest in certain uses of data. However, unitary theories fail to acknowledge the individual at all, and this is problematic if we consider as integral, the presence of a legitimate decision-making procedure for deciding cases of conflict; a procedure that must be justifiable to the relevant publics affected by a given type of processing.

Finally, in considering Held's work on the public interest, what is valuable is not only her typology of the concept, but her interpretation of the relationship between public and individual interests. Held acknowledges the undeniable *normative* element of the public interest, which explains the utmost importance of routine scrutiny of both commonly accepted understandings of what the public interest means in a particular context but also of transparent decision-making procedures. Her conception allows for justifiable conflicts between interests, something that is necessary in data protection, where decisions must be made that impact *both* the public interest in protecting informational privacy and in certain uses of personal data. Overall, the theoretical analysis undertaken has informed my development of key components to understanding the public interest concept in data protection, which are presented in Chapter 6.

Until now, the legal focus has been on the application of the public interest concept in data protection with the addition in this chapter of the often-overlapping context of Article 8 jurisprudence. Given the little case law and guidance on the public interest conditions it is prudent to expand our 'evidence base' and consider further examples of the public interest in cognate areas of law. The following chapter will examine how the public interest is deployed in the analogous legal contexts of freedom of information law, copyright and whistleblowing. From this analysis, we can further test the new conceptual understanding of the public interest being developed in this thesis and determine what is practically required to implement the public interest concept in law.

Chapter 5 Apples and Oranges? (In)consistencies of the Public Interest Concept in Freedom of Information, Copyright and Whistleblowing Law

1. Introduction

Considering the conclusions reached in Chapter 4, we may have to accept that the public interest is not capable of precise definition and that it may be *counter* to the public interest to claim to have defined it in a final sense. Nevertheless, is there not something that can be done to help address the uncertainty surrounding the concept in data protection? The forthcoming the GDPR poses greater requirements for obtaining valid consent while simultaneously broadening the definition of personal data, making it more difficult to rely on anonymisation.[636] The changing landscape will provide even greater incentives for practitioners and regulators alike to engage with the public interest conditions, hence the significance of my contribution of redeploying the public interest concept in a more accessible but theoretically and legally sound manner.

In this chapter I examine how the public interest has been implemented in cognate areas of law with greater and lesser 'success' in comparison to the uncertainty that surrounds the public interest conditions in data protection. This offers an opportunity to further refine our substantive understanding of the public interest as a concept while expanding the legal basis for developing a new approach to the public interest conditions in data protection. I will examine the operation and interpretation of the public interest test in freedom of information law, the public interest defence in copyright and the public interest test in whistleblowing law to determine:

[636] I have considered the impact of these changes (GDPR Art 7; Art 4(1) and Recital 26) as applied to the social sciences research context. Leslie Stevens, 'The Proposed Data Protection Regulation and Its Potential Impact on Social Sciences Research in the UK' (2015) 1 European Data Protection Law Review.

- What, if any, features of the public interest concept are common and can be generalised across these different legal domains?
- What features of the public interest are specific to these different legal contexts? (i.e. what features must be distinguished from data protection?)
- To what extent can the common features identified be applied to improve the deployment of the public interest concept in the data protection context?

The comparisons drawn in this chapter are justified on several grounds. First, each of these areas of law regulate the use of information which is 'protected' to greater and lesser extents. Second, within these domains the public interest acts either as an exemption or final point in consideration for applying the relevant legal provisions as to the use or disclosure of the information in question. Third, the public interest is not defined in any of these areas of law but is interpreted within regulatory and court decisions as well as in some instances in authoritative guidance.

I will first examine the successful deployment of the public interest test in freedom of information law as a close legal 'relative' to data protection, followed by consideration of the rather unsuccessful implementation of the public interest defence in copyright. The public interest test in whistleblowing is the final area of law analysed. Within each area of analysis, I will weave in relevant contrasts and comparisons to the data protection context. Overall, this chapter will demonstrate that the public interest *is* being used by actors in other legal fields and therefore is capable of being effectively implemented – it is not unreasonable that we might expect to use it successfully in the data protection context as well. I conclude by summarising a list of elements of the public interest which I have extracted from analysing these legal domains; these elements are capable of generalisation and therefore potentially applicable (and helpful) to understanding and applying the concept in data protection.

2. The Public Interest Test in Freedom of Information Law

In freedom of information law, the public interest plays a central role in determining whether a public authority is required to disclose information.[637] The aims of freedom

[637] Both freedom of information and data protection legislation implicate citizens' information rights. Data protection law regulates the handling of personal data, whereas freedom of information law is

of information law are important to understanding what the public interest encapsulates in this context. In the UK, freedom of information law is premised on the idea that citizens have a general right of access to information held by public authorities.[638] In freedom of information law, this general right to access is limited by a set of exemptions including for reasons of national defence,[639] international relations,[640] confidentiality[641] and the health and safety of individuals.[642] Exemptions from disclosure are either 'absolute'[643] or 'qualified'[644].

As to qualified exemptions, section 2(2)(b) of the FOIA 2000 and section 2(1)(b) of the FOISA 2002 provides that a public authority must still disclose information (even if a qualified exemption applies) unless in all circumstances the public interest in maintaining the exemption outweighs the public interest in disclosing the requested information. This is known as the 'public interest test'. Absolute exemptions are *not* subject to the public interest test which is 'testing' the public authority's *claim* that in all circumstances of the case, the public interest in maintaining the exemption outweighs the public interest in disclosure. As per, section 17 of the FOIA 2000 and section 16 of the FOISA 2002, the public authority must notify the requester of their refusal to disclose the information and state the reasons for this claim, for example if they

---

intended to promote transparency in government by making certain records available to the public. An important distinction is that freedom of information law does *not* give citizens the right to access their personal data; such requests must instead be made via a section 7 subject access request under the DPA 1998. Indeed, under s 40(1) of the Freedom of Information Act 2000 ('FOIA 2000') (and the Freedom of Information (Scotland) Act 2002 ('FOISA 2002'), s 38(1)(a)) requests for records which contain personal data of the requester must be treated as subject access requests under data protection law. Furthermore, under s 40(2) (and s 38(1)(b) in Scotland) an absolute exemption from disclosure exists for records containing personal data of third parties. Nevertheless, disclosure which is found compatible with data protection law is generally still possible i.e. the absolute exemptions do not equate to an absolute bar on disclosing personal data. See, for example, *House of Commons v Information Commissioner and Leapman, Brooke, and Thomas* (EA/2007/0060, 26 February 2008) where the Information Tribunal required disclosure of personal data even when this could cause significant harm and distress to the individuals involved (in this case, MPs and disclosures over their expenses).

[638] FOIA 2000, s 1(1) and FOISA 2002, s 1(1). The 'right of access' in data protection law cannot be directly equated as in data protection, access is always conditional upon the requirements of s 7 of the DPA 1998 being met.

[639] FOIA 2000, s 26 and FOISA 2002, s 31.

[640] FOIA 2000, s 27 and FOISA 2002, s 32.

[641] FOIA 2000, s 41 and FOISA 2002, s 36.

[642] FOIA 2000, s 38 and FOISA 2002, s 39.

[643] For example, there is an absolute exemption for reasons of confidentiality (s 41 FOIA 2000 and s 36 FOISA 2002) and for court records (s 32 FOIA 2000 and s 37 FOISA 2002).

[644] All exemptions not explicitly designated as 'absolute' per s 2(3) of FOIA 2000 and s 2(2) of FOISA 2002 are 'qualified'.

consider a qualified exemption to apply and that the public interest lies in maintaining the exemption.

As to enforcement, in England, Wales and Northern Ireland, the ICO is charged with enforcing the FOIA 2000. The ICO '…can overrule a public authority's application of the public interest test and form his or her own view of where the balance lies.'[645] In Scotland, the Scottish Information Commissioner ('SIC') is responsible for enforcing the FOISA 2002[646] and can similarly override a Scottish public authority's application of the public interest test on grounds that the authority has not dealt with a request in accordance with the requirements of Part I of FOISA 2002.[647] In England, Wales and Northern Ireland, the public authority (or requester) can appeal the Information Commissioner's decision to the First-tier Tribunal on Information Rights ('FTTIR') and onwards (in certain circumstances). In Scotland, appeals may be made to the Court of Session per section 56 of the FOISA 2002, which again may go further depending on the case.

With nearly a decade of decisions taken by the Information Commissioner, the SIC, and subsequent appeals to the FTTIR and Court of Session, a wealth of guidance has been produced on how the public interest test operates and is interpreted (unlike the dearth of guidance on the public interest conditions under the DPA 1998). Below I will consider potential reasons why the public interest has been more successfully implemented in the freedom of information context and what lessons might be learned for improving understanding and deployment of the concept in data protection. In the main, my analysis will focus on the public interest test as it applies and is interpreted regarding the FOIA 2000 but I will acknowledge, where relevant, important differences in the way the test is interpreted in Scotland.[648]

---

[645] Note: the ICO has authority over all UK-wide public authorities including when operating or based in Scotland. FOIA 2000, s 50; Megan Carter and Andrew Bouris, *Freedom of Information: Balancing The Public Interest* (Second, The Constitution Unit University College London 2006) 17.

[646] And other freedom of information legislation in Scotland including the Environmental Information (Scotland) Regulations 2004 and the INSPIRE (Scotland) Regulations 2009.

[647] FOISA 2002, s 47.

[648] For example, as to the interpretation of certain exemptions which seem to require a Scottish public authority to prove a higher standard of 'harm' if disclosure were to occur than under the FOIA 2000 (i.e. as to sections: 27(2)(b), 28(1), 30, 31(4), 32(1)(a), 33(1)(b), 33(2), 35, and 40). When claiming these exemptions, the FOISA 2002 requires that a Scottish public authority demonstrate that disclosure

2.1 A presumption for disclosure: the prioritisation of the public interests at stake in freedom of information law

As stated above, under section 2(2)(b) of the FOIA 2000, even where information has been properly found to be exempt under one of the qualified exemptions listed in Part 2 (such as the qualified exemption for trade secrets and commercially sensitive information in section 43), the duty to disclose continues unless, in all the circumstances, the public interest in maintaining the exemption *outweighs* the public interest in disclosing the information. The public interest test does *not* apply to any of the *absolute* exemptions[649] such as the exemption for parliamentary privilege (section 34).

Thus, unlike data protection where there are two (non-absolute) public interest aims of the legislation, section 2(2)(b) demonstrates that freedom of information law prioritises the *disclosure* of information. Indeed, the purpose of freedom of information law is '…to make provision for the disclosure of information held by public authorities.'[650] On this point the ICO's guidance on the public interest test provides that:

> If the public interest is equal on both sides, then the information must be released. If the public interest in disclosure is greater than the public interest in maintaining the exemption, then the information must also be released. In this sense, we can say that there is an assumption in favour of disclosure in FOIA.[651]

---

would or would be likely to 'prejudice *substantially*' the function of government involved. This contrasts with the equivalent provisions under the FOIA 2000 which only require that disclosure would 'prejudice' the government function in question. Therefore, where such exemptions are applied, *Scottish* public authorities would necessarily need to demonstrate a stronger case for maintaining the exemption as opposed to their English, Welsh and Northern Irish counterparts. Discussed in Carter and Bouris (n 645) 81.

[649] Except for section 41 of the FOIA 2000 where 'disclosure of information amounts to an actionable breach of confidence.' Discussed by Carter and Bouris: '…even though section 41 is not subject to a statutory public interest test, the question of public interest still forms part of the analysis as to whether disclosure of the information to the public would constitute an actionable breach of confidence under section 41(1)(b).' This is because of the equitable principles applicable to obligations of confidence which calls for a balance between the public interest in protecting confidentiality and the public interest in disclosure. Where the obligation of confidence arises 'at law', the Court would instead consider the rights between the parties as stipulated in the contract. ibid 23–24.

[650] FOIA 2000, Introductory Text.

[651] ICO, 'The Public Interest Test: Freedom of Information Act' (2016) 5 <https://ico.org.uk/media/for-organisations/documents/1183/the_public_interest_test.pdf>.

This prioritisation of the public interest in disclosure over any conflicting public interests (favouring *non*-disclosure) offers important *conceptual* clarity on the meaning of the public interest and balance to be struck between competing public interests in the freedom of information context. The difficulty in deciding conflicts between two public interests is partially lessened since from the outset one public interest is normatively understood to be privileged over another; where the balance is 'close' and there appears to be a 'tie' the privileged public interest must prevail. For example, consider the delicate balancing undertaken by the Information Commissioner in *The Complainant v the Department of Health (DoH).*[652] In this case the complainant requested a copy of the legal advice procured by the DoH on the application of competition law to a provision of the Health and Social Care Bill. The Information Commissioner found that although there was a 'very strong' public interest in public authorities receiving full and frank legal advice without the fear that it could be disclosed publicly, that any harm caused by disclosure did not ultimately outweigh the also 'very strong' public interests in favour of it.[653]

This finely balanced public interest determination in *The Complainant v the DoH* is one example where the prioritisation of disclosure can be seen even with strong public interests in favour of maintaining an exemption. Even if we acknowledge the numerous grounds upon which public authorities can *avoid* disclosure under Part II of the FOIA 2000, and thus the acknowledgement of the other public interests in the balance,[654] the legislation is unambiguous in the application of the public interest test that *disclosure* is privileged within this legal regime.

How does this contrast with the data protection context? No such prioritisation is found in the DPA 1998 or DPD. While the text of the DPA 1998 does not explicitly

---

[652] ICO, Decision Notice FS50402010 *Department of Health* (2011), reconsidered in ICO, Decision Notice FS50429566 *Department of Health* (2012) coming to the same conclusion.
[653] Decision Notice FS50429566 *Department of Health* (2012) [31]-[35].
[654] In the words of then Parliamentary Under-Secretary of State for the Home Department, Mr Mike O'Brien, during the Parliamentary Debate on the Freedom of Information Bill: '…the public interest is also served by some recognition of a right to privacy, some rights to commercial confidentiality and the right to develop an efficient policy advice system within Government—as well as the right to know.' HC Deb 7 December 1999, vol 340, col 788.

transpose the aims as provided in the DPD[655], the recitals to the Directive do stipulate that the purpose of data protection law is to protect informational privacy *and* facilitate the use of personal data.[656] This means that in data protection where there are strong public interests both in favour of and against the processing of personal data, and where the law is largely silent as to how to strike an appropriate balance between the two,[657] that it is not possible to determine in advance which interest should prevail. If a use of data is perfectly lawful, ethical and 'in the public interest', when might the interests of the data subject(s), a particular group or wider society nevertheless override this? If we also accept that there is a public interest in the protection of informational privacy there *are* surely circumstances where even if a use of data is necessary and in the public interest, the public interest in privacy may nevertheless require that data not be processed.

The way in which the public interest conditions are worded[658] does not offer any assistance here. There is no explicit balancing of interests required in the public interest conditions. And while the UK Courts have deferred to the procedural principles from European jurisprudence, on how key terms within the public interest conditions should be interpreted, there currently is no settled approach to 'balancing' in this context.[659] Things are arguably even more confused if we contrast the wording of the public interest conditions to the legitimate interests condition. Under the DPA 1998, Schedule 2 paragraph 6 (and the DPD Article 7(f)), a prioritisation *is* made between the legitimate interests of the data controller in processing versus any impact upon individuals. Where processing is 'unwarranted' and it prejudices the rights and freedoms or legitimate interests of the data subject(s), reliance on this condition would not hold.[660] In such

---

655 Only that it is 'An Act to make new provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information.' DPA 1998, Introductory Text.
656 DPD, Recitals 2-10.
657 Bar specific provisions such as in the DPD, Art 7(f) (and DPA 1998, Sch 2, para 6), where a data subject's rights and interests are prioritised over the data controller's legitimate interests in processing if '…the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.'
658 DPA 1998, Sch 2 para 5(d); DPPSPD 2000, Sch, paras 1-4, 9; DPD, Art 7(e); Art 8(4).
659 See Chapter 4 Section 3.2.3.
660 DPA 1998, Sch 2 para 6.

circumstances, the rights and interests of the data subject are prioritised over the legitimate interests of the data controller in processing.

When *would* the balance tip in favour of the data subject if the data controller can meet all the requirements of the public interest conditions? In other words, when is the processing of personal data *normatively* justifiable based on the public interest? Although to rely upon the public interest conditions processing must be 'necessary' and of a 'public nature', there remains no guidance on when the public interest in protecting informational privacy may nevertheless override a necessary, public interest use of data especially when it comes to *research use*s. A clearer indication of the circumstances where the protection of informational privacy or the use of data would be prioritised would help to alleviate some of this uncertainty.

2.2 The importance of function and perception: how the role of the public interest concept differs in freedom of information versus data protection

The public interest test is the subject of at least fifty-one FTTIR cases[661] and undertaken in up to 1,018 decisions by the SIC[662]. While the FTTIR cases are not directly comparable to the decisions by the SIC (given that the former represents a second external review versus the latter as a *first* external review) the plethora of decisions has facilitated the publication of comprehensive guidance by the ICO[663] and SIC on the public interest test[664]. As stated throughout this thesis, a key issue inhibiting the successful use and fuller understanding of the public interest concept in data protection is the dearth of case law and guidance on the public interest conditions. Two questions thus emerge:

---

[661] A search performed on the First-tier Tribunal on Information Rights website (on 26 September 2016) for cases implicating the FOIA 2000 on the subject of the public interest test provided a total of 51 decisions.
[662] A search performed on the SIC website (on 26 September 2016) for cases containing the exact phrase 'public interest test' filtering for decisions regarding only qualified exemptions (Sections 27-35, 36(1), 38(1)(b), 39-41) provided a total of 1,018 decision results cumulatively.
[663] ICO, 'The Public Interest Test: Freedom of Information Act' (n 651).
[664] Scottish Information Commissioner, 'The Public Interest Test in FOISA: Briefing' (2016) <http://www.itspublicknowledge.info/nmsruntime/saveasdialog.aspx?lID=9842&sID=684>.

- Why have public authorities more readily and regularly engaged with the public interest concept in the freedom of information context, as evidenced by the extensive case law examining public authorities' application of the public interest test?
- Why has the ICO chosen to provide comprehensive guidance on the public interest concept in the freedom of information context but not on the public interest conditions for processing under the DPA 1998?

Answers to these questions can reveal reasons why the role of the public interest conditions may have been marginalised and ultimately neglected in the data protection context. The insights gained from this analysis emphasises the important role played by the public interest conditions and thus the need for authoritative guidance.

The answer to both questions posed above arguably lies in the central role and function of the public interest concept in freedom of information law as opposed to the role of the concept *as perceived* by data controllers in data protection. Under freedom of information law, public authorities *must* engage with the public interest concept if they want to rely upon a qualified exemption to prevent disclosure of information under the FOIA 2000 or the FOISA 2002. This is because the public interest test operates as a final point of consideration in determining whether to uphold an exemption to disclosure under the legislation. This creates the ultimate incentive for a public authority to engage with the public interest concept; indeed, they have no other choice. As for the ICO's and SIC's provision of guidance, the public interest test plays such an integral role to the functioning of the legislation that it would be a dereliction of its duties to not provide guidance as both are required to promote observance of the FOIA 2000 and FOISA 2002, and disseminate guidance on best practice.[665]

In comparison, the public interest conditions are one of *several* lawful routes to legitimising the processing of personal data. Put simply, data controllers have more options – other routes to legitimising processing. As such it is arguable that the public interest conditions are not as integral to the functioning of the DPA 1998. This apparent marginalisation is compounded by the common misperception of data controllers that the public interest conditions are 'exemptions' from the need to obtain

[665] This is references section 47 'General functions of Commissioner' of the FOIA 2000 and section 43 'General functions of Commissioner' under the FOISA 2002.

consent; in other words, the public interest conditions are only relevant where consent is impracticable and disproportionate to obtain. As I have argued in Chapter 2, by misconceiving the public interest (and all other conditions for processing) as *exemptions* to obtaining consent, this perpetuates the current risk averse culture that narrows the legitimisation of research to the confines of consent or anonymisation, neglecting any potentially valid (and lawful) reliance on the public interest. The public interest conditions are *wrongly perceived* by data controllers (and arguably others including members of the public) as a marginal provision within the broader scheme of the DPA 1998 and thus not necessarily important enough to be used by data controllers or be the subject of dedicated guidance by the ICO.

To counter this, I would argue first that the conditions for processing, more generally, *are* integral components to the functioning of the DPA 1998. Consent and the other conditions will often *not* be relevant for research uses of data, in particular where research relies on the reuse of administrative data.[666] Here, the public interest conditions are relevant for public authorities to justify their own use and/or sharing of administrative data for research (while clearly, this condition cannot resolve issues related to the legality of reusing public sector data for purposes other than research).[667] Neither publicly beneficial research nor the use of data by public authorities can be ignored as trivial to the aims of data protection law; consider the significant attention paid to these forms of processing in the legislative history to the DPD.[668] The importance of the public interest conditions may be further underscored if we consider new provisions introduced by the forthcoming GDPR. Here the requirements for relying upon consent are significantly increased[669] whereas the circumstances in which a data controller can rely upon the legitimate interests provision are being tightened and may no longer be available to public authorities such as universities.[670] As such, the

---

[666] See Chapter 2 Section 4.
[667] For example, issues of incompatibility of processing may arise where administrative data are being shared for *non*-research purposes and thus cannot enjoy the benefits of Article 6(1)(b); in such circumstances consent may be the only appropriate legal basis, subject further to DPD, Article 13's exemptions. Stevens (n 636); Laurie and Stevens, 'Developing a Public Interest Mandate for the Governance and Use of Administrative Data in the United Kingdom' (n 63).
[668] See Chapter 3 Section 2.6.
[669] GDPR, Art 7-8.
[670] GDPR, Art 6(1)(f) which provides: 'Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.' On 7 August 2017, the UK

public interest conditions may play an enhanced role under the GDPR, without the necessary guidance to interpret it. Thus, to answer the two questions posed in the beginning of this section:

- Public authorities more readily and regularly engage with the public interest test in freedom of information law because they have no other choice but to do so when relying upon a qualified exemption; and
- The integral role of the public interest test to freedom of information law and the more regular engagement and reliance on it (and thus proliferation of decisions and case law interpreting its application) obliges the ICO and SIC to compile and disseminate best practice guidance on the issue.

As discussed above, despite the apparent marginalisation of the public interest conditions, these provisions do play an important role within the wider scheme of data protection law. Moreover, considering the forthcoming GDPR, these provisions are likely to be relied upon more often by public authorities, which in the UK includes universities (i.e. research producing institutions). Herein lies a renewed opportunity and call for the level of guidance the ICO has already provided in the freedom of information sphere.

2.3 The importance of authoritative guidance: the provision of action guiding principles and context specific examples

To conclude my analysis of the public interest test in freedom of information I will review key aspects of the guidance provided by the ICO and SIC. I will consider:

Government released a Statement of Intent for their release of the UK Data Protection Bill in September 2017. Within the annex to this, the position was taken that UK derogations will define 'public authorities' in line with the definition in FOIA 2000, which includes universities. This means that in the UK, that universities would *not* be able to rely on the legitimate interests condition (Article 6(1)(f) of the GDPR), making consent or the public interest condition the key alternatives for processing. Department for Digital, Culture Media & Sport, 'A New Data Protection Bill: Our Planned Reforms' (2017) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/635900/2017-08-07_DP_Bill_-_Statement_of_Intent.pdf>; Ruth Boardman, James Mullock and Emma Drake, 'The UK Government Publishes Its Statement of Intent for Data Protection Bill and GDPR' (*Bird & Bird*) <https://www.twobirds.com/en/news/articles/2017/uk/uk-government-publishes-its-statement-of-intent-for-data-protection-bill-and-gdpr>; 'Annex - Summary of GDPR Derogations in the Data Protection Bill' (2017) <https://webcache.googleusercontent.com/search?q=cache:vmMWzT2gNBkJ:https://www.twobirds.com/~/media/pdfs/summary-of-gdpr-derogations-in-data-protection-bill.pdf%3Fla%3Den+&cd=1&hl=en&ct=clnk&gl=uk&client=safari>.

- How have the ICO and SIC defined the public interest concept in freedom of information?
- To what extent would data protection law benefit from similar guidance?
- In what respects is the development of such guidance plausible in the data protection context?

2.3.1 Defining the public interest: context is key

During the Parliamentary Debates on the Freedom of Information Bill, the then Home Secretary, Mr Jack Straw, considered the range of public interests served through freedom of information legislation:

> The Bill will lead to cultural change throughout the public sector. There will be more information about how health authorities, local councils and the police deliver services. It will give citizens a right to know and a right to appeal to the commissioner if they do not get the information that they have sought. That is a fundamental change in the relationship between the citizens and the state.[671]

It is clear that Parliament was intent on ensuring that despite the numerous exemptions in the Freedom of Information Bill, that these would not ultimately prevent disclosure where it is in the public interest to do so.[672] To 'protect' disclosure they also ensured that the Information Commissioner as an independent arbiter would have the 'final' word on where the public interest lies,[673] and hence, that the Bill would become 'an effective weapon of modernising government and to make government more open, responsible and accountable to citizens.'[674] Although the public interest was not explicitly defined under the FOIA 2000 or FOISA 2002, Mr Straw's statements, as well as those within subsequent ICO and SIC guidance, give a clear indication of the conceptual contours of the public interest in the context of freedom of information law.

The ICO considers that the public interest in freedom of information '…can cover a wide range of values and principles relating to the public good, or what is in the best

[671] HC Deb 7 December 1999, vol 340, col 725.
[672] HL Deb 20 April 2000, vol 612, cols 823-93.
[673] HC Deb 7 December 1999, vol 340, cols 751-52; HL Deb 20 April 2000, vol 612, cols 838, 848, 860.
[674] HL Deb 20 April 2000, vol 612, col 884.

interests of society'. The ICO goes on to provide a non-exhaustive list of examples including:

> …there is a public interest in transparency and accountability, to promote public understanding and to safeguard democratic processes. There is a public interest in good decision-making by public bodies, in upholding standards of integrity, in ensuring justice and fair treatment for all, in securing the best use of public resources and in ensuring fair commercial competition in a mixed economy.

The ICO clarifies that even if these examples represent strong public interest reasons for disclosure, that the facts of each case must be examined to determine the appropriate balance between withholding information and disclosure. In sum 'This suggests that in each case, the public interest test involves identifying the appropriate public interests and assessing the extent to which they are served by disclosure or by maintaining an exemption.'[675] This reinforces the important point made in Chapter 4 that the public interest can never be exhaustively defined or determined in a final sense. Because the public interest is inherently context sensitive, what is in the public interest in one set of factual circumstances may not be in another. Nevertheless, it *is* possible to provide examples which typify the public interest in a particular context and derive principles from previous cases which can guide application of the term. This point is proven by the comprehensive guidance provided by both the ICO and SIC on the public interest test. The examples of relevant public interests, provided in the ICO's guidance, can be used to illustrate the reasonable range of interests relevant to the public interest test. How does this compare to the data protection context?

The DPD provides a list of public interest examples, but these are not all directly transposed into UK law; nor are they commonly accepted by the relevant publics or understood as public interest uses of data by data controllers.[676] More problematically, data controllers do not have an agreed procedure for assessing the public interest in their processing. A clear barrier to creating such a 'catalogue' of examples and a procedure for assessing the public interest in processing is that data protection lacks the significant body of case law and decisions that exist in the freedom of information

---

[675] ICO, 'The Public Interest Test: Freedom of Information Act' (n 651) 6.
[676] See Chapter 4, Section 3.1.

context. Nevertheless, as discussed in Chapter 3, the ICO *has* provided guidance on the application of the public interest concept in the section 32 exemption for journalism, literature and art, demonstrating the possibility of providing such advice for data controllers in context with the public interest conditions.

Turning to the SIC guidance, the SIC defines the public interest as follows:

> [The public interest] has been described elsewhere as 'something which is of serious concern and benefit to the public', not merely something of individual interest. It has also been described as 'something that is 'in the interest of the public', not merely 'of interest to the public.' In other words, it serves the interests of the public.[677]

Thus, for the SIC the ultimate question is: 'When applying the test, the public authority is deciding whether, on balance, it serves the interests of the public better to withhold or disclose information.'[678] And unlike the ICO guidance, the SIC considers how 'public' the public interest must be to successfully meet the required public interest threshold: 'The "public" in this context does not necessarily mean the entire population. It might relate to a relatively localised public (e.g. a small community or interest group) or to the wider public at large.'[679] This aspect of the SIC definition highlights an important feature of public interest theory examined in Chapter 4: the inherently contextual nature of the concept but also the importance of how you frame 'the public' when assessing the public interest in a particular matter.[680] The SIC rightly emphasises that 'the public' in the public interest will not necessarily refer to what is in the interests of the population as a whole; rather, how 'public' the public interest must be is determined by the relevant context of a particular case and especially in light of any impact caused to particular individuals, groups or wider society.[681]

How do these understandings of the public interest differ from what is understood of the concept in data protection? One critical difference is that in freedom of information

---

677 Scottish Information Commissioner (n 664) 1.
678 ibid.
679 ibid.
680 See Chapter 4 Section 4.1.2.
681 This approach to 'publics' echoes Article 8 jurisprudence of the ECtHR. See Chapter 4 Section 3.2.2.C.

law the private interests of the individual requesting the information '…are not in themselves the same as the public interest and what may serve those private interests does not necessarily serve a wider public interest.'[682] While this is a valid point and internally consistent with the aims of freedom of information law, this must be contrasted to the data protection context where the protection of *individual* informational privacy *is in itself a public interest*. It must be treated as such to remain consistent with the dual aims of data protection law and to ensure that the rights and interests of *many* (e.g. in a publicly beneficially form of data processing) are not always overriding the rights and interests of a few data subjects.[683] This highlights an important and generalisable feature of the public interest – that although the facts in every case may change, the *legitimate* interpretation of the public interest within a particular legal context, should be directed by the aims of the legislation in question:

> Indeed, the expression 'in the public interest', when used in a statute, classically imports a discretionary value judgment to be made by reference to undefined factual matters, confined only 'in so far as the subject matter and the scope and purpose of the statutory enactments may enable ... given reasons to be (pronounced) definitely extraneous to any objects the legislature could have had in view'[.][684]

Next I consider in more detail the practical aspects of the ICO and SIC guidance on the operation of the public interest test.

2.3.2 Factors to consider in the public interest test

As noted by the UK solicitor Estelle Dehon, addressing the public interest test in freedom of information law is not a matter of 'divining', but rather:

> There is now a rich framework of tribunal and court decisions within which decision-makers can operate to discern and evaluate the factors relevant to the public interest in disclosure and the public interest in maintaining the various exemptions. So, while the actual exercise of judgment may remain challenging,

---

[682] ICO, 'The Public Interest Test: Freedom of Information Act' (n 651) 7.
[683] Or, alternatively, that understandings of the public interest in processing are confined only to processing which benefits a 'preponderance' of individuals. Both ideas must be avoided. See Chapter 4 Section 4.1.1.
[684] *O'Sullivan v Farrer* (1989) HCA 61 [13], cited by Carter and Bouris (n 645) 5. Although this quote is from a High Court of Australia decision, this statement exemplifies the role often attributed to the public interest by the courts in common law jurisdictions.

> it is a task at which decision-makers, and their advisers, should become increasingly adept.[685]

Those navigating the public interest conditions in data protection have reason to be jealous of their freedom of information colleagues. Not only has the ICO and SIC guidance attempted to define the conceptual contours of the public interest, both have outlined 'relevant' and 'irrelevant' factors for public authorities to consider (or disregard) when addressing the public interest test. While the public interest must be considered in context, certain principles or factors *can* be generalised to help decision-makers take public interest decisions in the first instance as they must do in both the data protection and freedom of information contexts. Both the ICO and SIC created its guidance based on decisions and case law where the public interest test has been addressed, outlining factors that were considered to support an exemption or disclosure. Below I consider the key factors the ICO and SIC have extracted from the wealth of decisions they have taken and from case law.

2.3.2.A Arguments for and against disclosure – the Information Commissioner's Office Guidance

I have created the table below, which outlines a non-exhaustive list of factors that the Information Commissioner considered 'relevant' or 'irrelevant' to the application of the public interest test.[686]

Table 1

Relevant Factors	
Public interest in favour of disclosure	**Public interest in maintaining the exemption**
Transparency	Arguments must be context specific to the exemptions claimed; no general public interest arguments
Public interest in the issue	Public interests may be aggregated if several

[685] Estelle Dehon, 'Divining the Public Interest' (2016) 12 Freedom of Information 8, 10.
[686] ICO, 'The Public Interest Test: Freedom of Information Act' (n 651) 9–21.

	exemptions are claimed
Public interest in the information	
Suspicion of wrongdoing	
Presenting a full picture	
Irrelevant Factors	
Identity of requester	
Private interests of requester	
Information may be misunderstood	
Other means of scrutiny	
Interests of people in other countries	

While the substance of the arguments for and against disclosure is not necessarily relevant to the data protection context, the way these factors were evaluated by the Information Commissioner is. In considering this list of factors, the ICO has focused on providing a list of the principles underlying certain arguments e.g. the public interest in presenting a full picture of an issue where more specified examples are given and then a specific case is referenced in order to illustrate the principle in action.[687] A further noteworthy observation is that the factors in favour of maintaining an exemption are fewer (consistent with the prioritisation of disclosure under the legislation) and are not substantively defined. Here the ICO has directed the reader of its guidance to the appropriate procedure.

As to the appropriate procedure for applying the public interest test, public authorities must support their case for maintaining an exemption with arguments *specific to* the public interests involved regarding the particular exemption claimed.[688] For example, if arguing that the qualified exemption in section 27 of the FOIA 2000 applies, the public

[687] For example, as to an argument in favour of disclosure, that the information would present the full picture, the ICO specifies that 'For example, this may well be a public interest argument for disclosing advice given to decision makers. The fact that the advice and the reasons for the decision may be complex does not lessen the public interest in disclosing it and may strengthen it.' The ICO then illustrates the principle further by presenting a FTTIR case note on *Cabinet Office and Christopher Lamb v Information Commissioner*. The case concerned a request for Cabinet meeting minutes where the Attorney General's advice on the Iraq war was discussed. In deciding that the minutes should be disclosed, 'the majority considers that the value of disclosure lies in the opportunity it provides for the public to make up its own mind on the effectiveness of the decision- making process in context.' EA/2008/0024 AND EA/2008/0029 (2009) [82].

[688] Based on *Christopher Martin Hogan and Oxford City Council v Information Commissioner* ('*Hogan*') EA20050026 and 0030 (2006) [59] cited with approval in ICO, Decision Notice FS50488117 *Ministry of Justice* (2013) [26]-[27].

authority must assert specific reasons why disclosure would prejudice, or would likely prejudice, the relations between the UK and a particular state. In such a case, it would be irrelevant that disclosure would also prejudice the formulation of government policy unless the section 35 exemption was also being claimed. The guidance alerts public authorities to the stricter scrutiny of their public interest claims for maintaining an exemption:

> While the public interest considerations against disclosure are narrowly conceived, the public interest considerations in favour of disclosure are broad-ranging and operate at different levels of abstraction from the subject matter of the exemption.[689]

This stricter scrutiny is made clear when considering the more extensive and broadly construed list of factors in favour of disclosure. Also indicative of the high standard to meet are the factors which are considered 'irrelevant' or should be disregarded when applying the public interest test; these 'irrelevant' factors include, for example, the extent to which other public authorities might be able to provide scrutiny and oversight on the situation, and the motivations of the requester and thus the potentially vexatious nature of the request.[690]

In addition, the ICO's explanation of how to attach weight to the public interest arguments for or against disclosure is instructive.[691] Factors that may tip the balance in one way or the other include: 1) the likelihood of prejudice to occur to the public authority; 2) the severity of that prejudice; 3) the age of the information; 4) the nature of the specific information and public interest in disclosure; and 5) whether the information is already in the public domain. More generally as to the 'weighting' process, the ICO provides that:

> Once the public authority has identified the relevant public interest arguments for maintaining the exemption and for disclosure, it must then assess the relative weight of these arguments, to decide where the balance of public interest lies. This is not an exact process, but the authority should try to approach it as *objectively* as possible. If the Commissioner is dealing (sic) the case, we will consider these arguments, or consider other public interest

[689] *Hogan* (n 688) [60].
[690] ICO, 'The Public Interest Test: Freedom of Information Act' (n 651) 16–20.
[691] ibid 22–26.

> arguments that the authority did not include, and may reach a different conclusion.[692]

Although this is hardly explicit, the Information Commissioner is indicating the standard to which they will evaluate a public authority's application of the public interest test; that their claims will be evaluated on an *objective* rather than subjective basis. In other words, the Information Commissioner might ask: are the public authority's claims that disclosure would, or would likely, prejudice them, the government or the public, an *objectively reasonable* claim? This passage also alerts the public authority to the fact that the Information Commissioner will consider the public interest test *de novo* without deference to the public authority's own findings. Thus, it is in their best interests to identify and document their consideration of the public interest on both sides and as objectively as possible. The prospect of an objectively reasonable standard being applied, *de novo* review and the clear prioritisation of disclosure supported elsewhere in the guidance (and in the legislation), provides public authorities with an unambiguous steer on the way in which their decisions to not disclose information will be evaluated.

In considering this section, taken together with the other guidance provided, the ICO goes some way to providing public authorities a principled basis for applying the public interest test to their own circumstances. They have prescribed an approach capable of application by public authorities in a way that is consistent and internally coherent with the aims of freedom of information law. Their guidance can be said to instil confidence in decision-makers; confidence that they can apply the public interest test robustly as they are aware of the standards which will apply if the Information Commissioner reviews their decisions. As argued in Chapter 4, even if we have a descriptive understanding of the public interest – in the form of examples – to make a *legitimate* public interest determination on subject matter beyond these factual confines, decision-makers need criteria to assess the public interest in their own context. In considering the entirety of the ICO guidance on the public interest test, I would suggest that the following set of principles have been provided to guide public authorities when

---

[692] ibid 22 (emphasis added).

applying the public interest test to their own freedom of information circumstances. These principles are represented in the table on the following page.

Table 2

Prioritisation of disclosure	The primary purpose of freedom of information law is to facilitate the disclosure of public-sector information. The duty to disclose continues unless the public interest in maintaining an exemption *outweighs* the public interest in disclosure.
The public interest v what interests the public	The public interest can cover a broad range of values and principles related to the public good, but should be distinguished from what *interests* the public.
Context sensitivity	Even if certain public interests are inherent to matters related to freedom of information, such as the public interest in transparency and accountability, their presence are not dispositive. The public interest in disclosure and in favour of maintaining an exemption must always be examined in context of each case.
Identify and document public interest determination	Public authorities must identify the public interests in favour of disclosure and in favour of maintaining the exemption – there are always arguments to be made on both sides and these must be considered as objectively as possible. Public authorities should document their consideration of these issues.
Narrow understanding of the public interests in favour of non-disclosure	Whereas the public interests in favour of maintaining an exemption must be construed narrowly, the public interests in favour of disclosure can be more broadly understood. Arguments in favour of maintaining an exemption must be specific to the exemption(s) claimed.
In the event of a 'tie', disclosure prevails	Once the public interests on both sides have been identified, and appropriate weight given to the different factors at issue, if the balancing seems equal, disclosure must prevail.

While these principles are generic, when coupled with the more detailed list of relevant and irrelevant factors (with even more detail added by their reference to specific cases), public authorities are well equipped apply the public interest test without the

uncertainty which plagues application of the public interest conditions in data protection law. Below I will briefly consider how the SIC guidance differs and contributes to Scottish public authorities' understanding of the public interest test in freedom of information law in Scotland.

2.3.2.B Arguments for and against disclosure – the Scottish Information Commissioner's Guidance

I have created the following table, which outlines a non-exhaustive list of factors the SIC has considered 'should' or 'should not' be relevant when a Scottish public authority applies the public interest test; these are based on decisions taken by the SIC.[693]

Table 3

Factors which should be taken into account		**Factors which should *not* be taken into account**
Public interest in maintaining the exemption	**Public interest in favour of disclosure**	
Disclosure would impact negatively on safeguarding national security or international relations	General public interest that information is accessible	Embarrassment to Government or Public Officials
Disclosure would impact negatively on an individual's right to privacy	Disclosure contributing to the administration of justice and enforcement of the law	The 'seniority' of officials involved
	Ensuring effective oversight of public expenditure and that the public obtain value for money	Potential loss of confidence in Government or specific public authorities
	Public adequately informed of dangers to public health, safety or environment	Risk of the requester misinterpreting the information once received
	Ensuring public authorities adequately discharge their duties	
	Ensure fairness in regards to applications, complaints, reveal malpractice or correct misleading claims	
	Contribute to debates on matters of public interest	

[693] Scottish Information Commissioner (n 664) 3–4.

The SIC has provided a more descriptive list of factors which can be contrasted to the broader list of principles provided by the ICO. Despite being more descriptive, the SIC makes clear that 'This is not an exhaustive list, but gives an indication of the sort of issues authorities should be considering.'[694] Whereas the ICO guidance refers to the apparently 'inherent' public interest in transparency (in favour of disclosure) or in preventing 'prejudice' (in favour of non-disclosure) no such categorical statements are made within the SIC guidance as to any example of the public interest. What is of great value is the SIC's detailed guidance on each of the qualified exemptions, where they reference cases where both disclosure and non-disclosure prevailed. For example, consider the guidance as to section 27 of the FOISA 2002 which provides a qualified exemption from disclosure on the basis that 1) a public authority plans to publish the information within the next 12 weeks or 2) a university has obtained information in, or derived from, a 'programme of research', provided they are planning to publish the research.[695] The guidance poses key questions that a public authority should consider when seeking to maintain this exemption. Thus, the SIC appears to offer more contextually-based considerations than the ICO, which is helpful for public authorities in identifying the specific public interest arguments in favour of maintaining particular exemptions.

A further contrast is that the SIC guidance does not explicitly state that the public interests favouring non-disclosure must be narrowly construed (as provided in the ICO guidance [696]). However, a high threshold still clearly applies to Scottish public authorities who wish to withhold information based on several of the qualified exemptions.[697] Under certain exemptions, Scottish public authorities must demonstrate that the prejudice from disclosure would be 'substantial'. [698] Carter and Bouris consider that ' …making the exemption provisions in the Scottish FOI Act more difficult to satisfy… a likely result [is] that more information will be released under the Scottish

[694] ibid 3.
[695] Scottish Information Commissioner, 'Information Intended for Future Publication' <http://www.itspublicknowledge.info/Law/FOISA-EIRsGuidance/section27/Section27.aspx>.
[696] ICO, 'The Public Interest Test: Freedom of Information Act' (n 651) 11.
[697] FOISA 2002: s 27(2)(b); s 28(1); s 30; s 31(4); s 32(1)(a); s 33(1)(b); s 33(2); s 35; s 40.
[698] ibid.

legislation than will be the case under the UK legislation.'[699] If we consider that the primary aim of freedom of information law is to provide citizens with a general right to access public authorities' records, it is arguable the SIC's handling of qualified exemptions is something to be emulated within the rest of the UK.

2.4 Generalisable and distinguishing features of the public interest in freedom of information law

Much can be learned from the way in which the public interest test has been successfully deployed in the freedom of information context. The ICO and SIC have created comprehensive guidance on the public interest test arguably providing the maximum amount of detail and guidance possible for a determination as inherently context sensitive as the public interest is. The ICO's approach has been to provide a more principled basis for understanding the operation of the test; defining an approach that is more generally applicable to a wide variety of factual circumstances. In contrast, the SIC provided more succinct guidance on the public interest test with a detailed analysis of each exemption; this too is of great value when considering that the public interest must always be examined within the relevant context and facts of each case. Combining the set of principles provided in the ICO guidance with the context-based analysis of each exemption by the SIC, provides an exemplar of guidance on the implementation of the public interest concept. Admittedly, decisions on the public interest test in freedom of information law are not taken in this hybrid manner. However, in the analogous context of data protection, with the dearth of case law and guidance on the public interest conditions, there is an opportunity to develop and take such an approach which is made possible by the current activities and capabilities of the ICO. [700]

The ICO already conducts voluntary 'advisory visits' to data controllers across the UK.[701] During these visits the ICO provides '…practical advice to organisations on

[699] Carter and Bouris (n 645) 81 (emphasis added).
[700] In Chapter 6 I propose various 'solutions' to the dearth of guidance and interpretation of the public interest conditions.
[701] 'Advisory Visits' (*ICO*, 2016) <https://ico.org.uk/for-organisations/improve-your-practices/advisory-visits/>.

how to improve data protection practice. It normally involves a one-day visit from the ICO and a short follow up report.'[702] Alongside such advisory visits, which proactively support and promote good data protection practices, the ICO also provides data controllers with the opportunity to apply for more formal audits of their information handling practices[703] and undertakes various enforcement actions.[704]

These engagements activities are not only about what the organisations receive. From these activities, the ICO obtains rich information on data controller practices, from which they can document the types of contexts in which the public interest conditions are most relevant and typically arise. The ICO is therefore in a prime position to extract the broader principles that should govern an approach to the public interest conditions. These interactions would also allow the ICO to offer more contextualised guidance with examples on the applicability of the conditions in specific sectors by drawing upon its experience in working with a wide range of data controllers. Under section 51 of the DPA 1998 the ICO is already obliged to develop and disseminate codes of practice. As argued in Chapter 2, guidance on alternatives to consent or anonymisation, which would include the public interest conditions, is long overdue. Even though such engagement activities are clearly already part of the ICO's mandate, I suggest that the incentive to engage with data controllers in this way and provide this guidance will only increase because of the GDPR (and later, Brexit), whereby the public interest conditions will have increased relevance for a variety of processing contexts and data controllers.

In contrast to the rather successful use of the public interest concept in freedom of information law, in the section below I consider the public interest defence in copyright. Despite a series of landmark cases on the issue, the public interest defence in copyright remains subject to significant uncertainty as to its scope and legal status.

---

[702] ibid.
[703] 'Audits' (*ICO*, 2016) <https://ico.org.uk/for-organisations/improve-your-practices/audits/>. The ICO conducts 'audits' to offer more formal assessments of whether an organisation is following good data protection practice.
[704] 'Action We've Taken' (*ICO*, 2016) <https://ico.org.uk/action-weve-taken/>. Including enforcement notices, monetary penalties, undertakings and prosecutions.

3. The Public Interest Defence in Copyright Law

A common law defence to a claim of copyright infringement is that the unlicensed use of a protected work is allowable on public interest grounds. Section 171(3) of the Copyright, Designs and Patents Act 1988 ('CDPA') stipulates that Part I of the CDPA will have no impact on '…any rule of law preventing or restricting the enforcement of copyright, on grounds of public interest or otherwise.'[705] Section 171(3) does not further define the scope of this 'defence'. Indeed, the defence predates the CDPA. The public interest defence was originally developed in a series of cases involving both claims of copyright infringement and breaches of confidence where the public interest in disclosure was considered to outweigh the public interest in protecting the intellectual property and confidentiality of the information in question.[706] The public interest defence in copyright is best understood as '…a defence sitting outwith the statutory regime that would justify the publication of copyright material in certain circumstances.'[707] Thus it can be distinguished from the range of statutory permitted acts which allow the use of copyrighted material for particular purposes, such as for research[708], news reporting[709] and more recently caricature, parody and pastiche[710].

The role of the public interest concept is seemingly vaguer and more limited in copyright than in other areas of law such as whistleblowing (examined below) and freedom of information. The public interest is not integral to interpreting copyright law but instead provides a 'failsafe' defence for alleged copyright infringers who cannot otherwise defend their use of protected works. In this more limited role, the public

---

[705] Copyright, Designs and Patents Act 1988 (CDPA), s 171(3).
[706] Notably including *Beloff v Pressdram* [1973] 1 All ER 241 and *Lion Laboratories Ltd v Evans* [1985] QB 526. As examined in Gillian Davies, *Copyright and the Public Interest* (2nd edition, Sweet & Maxwell 2002); *Copinger and Skone James on Copyright* (17th edn, Sweet & Maxwell 2016).; on *Lion*: 3-432, 3-436, 21-107.
[707] Robert Burrell and Allison Coleman, 'The Public Interest Defence', *Copyright Exceptions: The Digital Impact* (CUP 2005) 80.
[708] CDPA, s 29. Research and private study are permitted acts but they must be for non-commercial purposes and provide appropriate acknowledgement.
[709] CDPA, s 30(2). This applies to the reporting of current events so long as appropriate acknowledgement is given. Acknowledgement is not required where the reporting is by sound recording or film.
[710] In October 2014, the UK Government added 'caricature, parody and pastiche' to the list of permitted acts in the CDPA, Section 30(a). These were 'optional' exceptions in under the Information Society Directive i.e. it was permissible but optional for Member States to implement these. (Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001), Art 5(3)(k).

interest defence offers courts an uncertain scope of discretion in their enforcement of copyright, to ensure that it does not run counter to an overriding 'public interest'. The question is, does the law sufficiently define what sorts of public interests may outweigh a '…copyright owner's right to peaceful enjoyment of his/her property'[711] and the conditions where this defence would be successful? What comparisons can be made to the data protection context and what might be learned from the uncertainty which surrounds the public interest defence?

3.1 The evolution of the public interest defence at common law

To understand the current uncertainty surrounding the defence and any relevant lessons for data protection, it is important to trace the key elements of the defence as it developed at common law.

The public interest defence in copyright was initially developed in the case of *Beloff v Pressdram*.[712] In *Beloff*, Mr Justice Ungoed-Thomas explained that the public interest defence was available in copyright because of its role as a general principle of common law rather than being a defence specific to copyright, such as fair dealing.[713] He did not provide that the defence would be available in *all* copyright right cases, only that it was available as a 'tool' to the Courts as it would be in any case. The public interest defence was to be limited to disclosures of copyrighted material that revealed illegal or otherwise immoral behaviour including:

> …matters carried out or contemplated, in breach of the country's security, or in breach of law, including statutory duty, fraud, or otherwise destructive of the country or its people, including matters medically dangerous to the public; and doubtless other misdeeds of similar gravity.[714]

---

[711] John Bowers QC and others, 'Whistleblowing and Copyright', *Whistleblowing: Law and Practice* (OUP 2012) 308.
[712] *Beloff* (n 706). The origins of the public interest defence is considered in more detail by Robert Burrell, 'Defending the Public Interest' [2000] European Intellectual Property Review 394, 400–403; Alexandra Sims, 'The Denial of Copyright Protection on Public Policy Grounds' (2008) 30 European Intellectual Property Review 189, 189–191; Jonathan Griffiths, 'Pre-Empting Conflict – a Re-Examination of the Public Interest Defence in UK Copyright Law' (2014) 34 Legal Studies 76, 79.
[713] *Beloff* (n 706) [259].
[714] ibid [260].

This narrow conception of the public interest defence can be traced back to the breach of confidence case *Gartside v Outram* where the defence was limited to cases where disclosure would expose *iniquity*: '… there is no confidence as to the disclosure of iniquity. You cannot make me the confidant of a crime or a fraud'.[715] Although it is not the purpose here to further analyse the defence in breach of confidence, it is important to acknowledge that the defence in copyright *arose out of* the reasoning applied in breach of confidence cases including in particular *Gartside*, *Initial Services Limited v Putterill* and *Fraser v Evans*.[716] The application of breach of confidence reasoning to the copyright context would later contribute to the uncertainty surrounding the scope of the defence in copyright.

3.1.1 A broader public interest defence: *Lion Laboratories Ltd v Evans*

By 1985, the public interest defence in copyright had seemingly evolved from the narrow parameters of its birth in *Beloff* while leaving important questions relating to the scope of the defence unanswered.

In *Lion Laboratories* Lord Justice Griffiths broke away from this narrower scope of the defence. *Lion Laboratories* was a case involving whistleblowing (a topic to be discussed in Section 4 below), where a manufacturer of breathalyser devices was claiming both breach of confidence and copyright infringement. Their former employees removed internal memoranda which questioned the reliability of the plaintiff's breathalyser devices and these were subsequently disclosed to the press. Although the documents were confidential and protected by copyright, the plaintiff's interlocutory injunction was overturned. It was deemed in the public interest to expose the unreliability of the devices given the potential for wrongful convictions of drink-driving. While failing to distinguish between the scope of the defence in breach of confidence versus in copyright, Lord Justice Griffiths explicitly stated that the public interest defence was *not* limited to matters of iniquity (as provided in *Beloff*):

> I am quite satisfied that the defence of public interest is now well established in actions for breach of confidence and, although there is less authority on the point, that it also extends to breach of copyright…I can see no sensible reason

[715] *Gartside v Outram* (1857) 26 Ch 113 [114].
[716] *Gartisde* (n 715); *Initial Services Limited v Putterill* [1968] 1 QB 396; *Fraser v Evans* [1969] 1 QB 349.

> why this defence should be limited to cases in which there has been wrongdoing on the part of the plaintiff…*it is not difficult to think of instances where, although there has been no wrongdoing on the part of the plaintiff, it may be vital in the public interest to publish a part of his confidential information*.[717]

It seems that the Court was attempting to strike a balance between the various public interests at stake, including 1) protecting the rights of copyright holders, 2) maintaining confidentiality between an employer and their employees and 3) the public interests served through disclosure. In this case, preventing the possible miscarriage of justice through disclosure was considered to outweigh the other public interests at stake, not least because of the potential for false positives on the faulty breathalysers which raised '…a serious question concerning a matter which affects the life, and even the liberty, of an unascertainable number of Her Majesty's subjects'.[718]

Nevertheless, the judgment in *Lion Laboratories* provided little that could be *generalised* when considering the applicability of the defence in other copyright cases; that is, other than the fact that the defence would *not* be limited to cases where the copyright holder is guilty of some wrongdoing. The Court failed to clarify the boundaries between the defence in copyright versus in breach of confidence. Is the defence available in all copyright cases (as in breach of confidence) or just part of the Court's inherent discretion to refuse an injunction?[719] This question remained unanswered as the Court conflated consideration of the public interest in copyright and in confidentiality as the public interest in *confidential information*:

> The first public interest is the preservation of the right of organisations, as of individuals, to keep secret confidential information. The courts will restrain breaches of confidence, and breaches of copyright, unless there is just cause or excuse for breaking confidence or infringing copyright.[720]

The Court further failed to address the range of reasonable and permissible public interests that may outweigh the interests of a copyright-holder in any given case, only to provide that '…"[iniquity] is merely an instance of just cause or excuse for breaking

---

[717] *Lion Laboratories* (n 706) [550] (emphasis added).
[718] ibid [546].
[719] A question raised by Griffiths (n 712) 80.
[720] *Lion Laboratories* (n 706) [536].

confidence.'" [721] Lord Justice Stephenson did place certain limitations on the applicability of the defence including '…(i) that it would only apply where disclosures genuinely served the public interest and (ii) that it would generally only cover disclosures to the appropriate authorities rather than to the public at large'.[722] Without further defining what types of disclosures would genuinely serve the public interest in the context of copyright (as opposed to breach of confidence) this reasoning did not improve understandings of the range of public interests that could be relevant to consider in copyright infringement. As discussed in Section 2.4 above, regarding freedom of information law, the provision of examples of the public interest *coupled with* relevant principles or criteria can better support decision-makers' application of the public interest in a particular context – something which seems lacking in copyright (and data protection).

3.1.2 One step forward and two steps back: the narrowing of the public interest defence in *Hyde Park* and *Ashdown*

The scope of the defence was later significantly narrowed in *Hyde Park Residence Ltd v Yelland*[723] where the Court of Appeal ruled that the CDPA did *not* provide a generally applicable public interest defence to copyright infringers.[724] The facts surrounding *Hyde Park* are well known as they relate to claims of copyright infringement and breach of confidentiality in regards to still images from security footage capturing Diana Princess of Wales and Mr. Dodi Fayed the day before their deaths in 1997.[725] Copies of these images were given to a reporter at *The Sun* from a security guard who worked at the villa where the security footage was originally captured. *The Sun* defended publication based on fair dealing under section 30(2) of the CDPA and that publication was not unlawful because it was in the public interest. Mr Justice Jacobs upheld both these defences and dismissed the claim.

---

[721] *Lion Laboratories* (n 706) [537].
[722] Griffiths (n 712) 80.
[723] *Hyde Park Residence Ltd v Yelland* [2000] 3 WLR 215 ('*Hyde Park II*').
[724] ibid [43] (Aldous LJ).
[725] *Hyde Park Residence Ltd v Yelland and others* [1999] EWHC Patents 247 ('*Hyde Park I*').

On appeal, the Court reversed this judgment concluding that neither a defence based on fair dealing or the public interest could succeed.[726] Of relevance to the discussion here is how Lord Justice Aldous interpreted the scope of the public interest defence. Seemingly reverting to the narrow scope in *Beloff*, he stated that section 171(3) of the CDPA merely acknowledged a court's inherent jurisdiction to refuse to enforce an action for infringement if it would be contrary to public policy.[727] Thus it would seem the public interest, at least in terms of this 'defence', had no independent meaning from the defence more generally available at common law. The Court of Appeal endorsed this narrower version of the defence, where it would be applicable only if wrongdoing would be prevented and or revealed through disclosure:

> …a court would be entitled to refuse to enforce copyright if the work is: (i) immoral, scandalous or contrary to family life; (ii) injurious to public life, public health and safety or the administration of justice; (iii) incites or encourages others to act in a way referred to in (ii).[728]

Lord Justice Aldous argued this on a principled basis; that the statutory nature of copyright law versus the judicial origins of breach of confidence made it inappropriate for the courts (in cases of copyright infringement) to subvert the clear intentions of Parliament to limit the use of protected works to those permitted in the CDPA.[729] He considered that these permitted acts '…would therefore appear to set out in detail the extent to which the public interest overrides copyright' and on this basis it would be inappropriate for the Court to disrupt this carefully constructed balance between copyright and other public interests.[730]

Moreover, Lord Justice Aldous considered this narrower form of the defence more appropriate for copyright (than the broader form in breach of confidence) because: '(i) copyright protected only form, and not underlying facts or ideas, and (ii) international copyright treaties did not permit the maintenance of a broad "public interest" principle.'[731] In his concurring opinion, Mance LJ distinguished reasons why the

---

[726] *Hyde Park II* (n 683) [40], [67] (Aldous LJ).
[727] ibid [44].
[728] ibid [66].
[729] ibid [43].
[730] ibid.
[731] Griffiths (n 712) 82.

broader form of the defence is acceptable and appropriate in the breach of confidence context versus in copyright. As to breach of confidence, Lord Justice Mance provides that:

> Confidential information is information about A's affairs which B possesses, but in respect of which B may owe A a duty not to disclose the information to others. Confidence and secrecy on the one hand and disclosure and publication on the other lie at opposite ends of one and the same continuum. Protection of confidence depends on the force of A's interest in maintaining secrecy. Freedom to publish depends on the force of competing considerations such as the public interest in knowing the truth.[732]

He then contrasts this to copyright:

> Copyright is by contrast a property right, conferring on A alone the exclusive right to do certain acts in relation to certain works including sound recordings and films. It protects the form of such works and not any information which they contain as such. And it is regulated by statute. Section 30 of the Act of 1988 expressly allows fair dealing with certain works for the purpose of criticism or review or of reporting current events. Copyright does not lie on the same continuum as, nor is it the antithesis of, freedom of expression. *The force of an owner's interest in the protection of his copyright cannot be weighed in the same direct way against a public interest in knowing the truth.*[733]

On this reasoning, Lord Justice Mance considered that the range of public interests that could legitimately outweigh the rights of a copyright holder should be interpreted *narrowly* because the CDPA had already 'spoken' on this issue (i.e. in its explicit provision of permitted acts). The different purpose and nature of rights and interests at stake in copyright versus breach of confidence cases meant that the public interest concept was intended to play different roles. Although, it should be noted, that Lord Justice Mance could not define the precise circumstances in which the public interest *could* legitimately play a role in copyright.[734]

---

[732] *Hyde Park II* (n 683) [75] (Mance LJ).
[733] ibid [76] (emphasis added).
[734] Mance LJ stated: '…the circumstances in which the public interest may override copyright are probably not capable of precise categorisation or definition.' ibid [83].

3.1.3 Narrow versus broad approaches to interpreting the public interest

A comparison, or rather *clarification* should be made at this juncture as it pertains to arguments for and against 'broad versus narrow' interpretations of the public interest concept. In *Hyde Park II* we see that the Court of Appeal interpreted the list of permitted acts under the CDPA as Parliament explicitly (and exhaustively) defining the circumstances in which other public interests may outweigh copyright. A similar argument can be imagined in the data protection context by someone opposed to a broad interpretation of the public interest conditions. One might argue that the DPA 1998 already provides a significant 'list' of public interests uses of data that are to greater and lesser extents exempt from various provisions of the legislation.[735] Furthermore, if we are to take account of the examples of public interest processing provided under the DPD, cumulatively, those might be the only plausible uses of data that could be justified based on the public interest. In the often-overlapping context of Article 8 of the ECHR, the ECtHR has found that a Member State's interference with an individual's rights must relate to one of the legitimate aims enumerated in Article 8(2).[736]

To counter such arguments for the data protection context, first consider that Schedule 2 paragraph 5(d) of the DPA 1998 provides an explicit and lawful ground for processing personal data based on the 'public interest' which may be availed by 'any person', clearly defining the relevant conditions that must be met to rely upon it. Compare this to section 171(3) of the CDPA which seems to only reiterate what was already true at common law – that no court would have to enforce a copyright if enforcement would run counter to opposing (and greater) public interests. Indeed, section 171(3) was introduced to ensure that the public interest defence at common law would be maintained and not eroded (even accidentally) by the CDPA.[737] Furthermore, section 171(3) does not provide in any detail what circumstances might

[735] For example, processing personal data only for the 'special purposes', which include journalism, literature and art, is exempt from complying with all but the seventh data protection principle so long as certain conditions are met. DPA 1998, s 32.
[736] See Chapter 4 Section 3.2.2.A.
[737] HL Deb 23 February 1988, vol 493, col 1162.

give rise to a valid public interest defence, potentially indicating that this is a matter ultimately decided by the courts on a case-by-case basis, not something for individual decision-makers to engage with. In contrast, data protection legislation indicates the relevant procedural conditions so that data controllers may rely on the public interest conditions i.e. processing must be 'necessary', 'for the exercise of any other functions of a public nature' and 'in the public interest'.

A second counter argument can be made based on the relevant legislative history. As revealed in Chapter 3, the *travaux* to the DPD clearly demonstrated that the public interest provisions and examples given in the recitals were merely examples and *not* an exhaustive list of public interest uses of data.[738] The way in which the UK Parliament transposed these provisions into the DPA 1998 was done without any reference to these examples, arguably leaving this determination even more open to interpretation in the UK, including by data controllers who could interpret the public interest concept within their relevant context. Moreover, the 'examples' of public interests given in the DPD were included only because these were lobbied for by particular Member States.[739] They were added to the DPD without any reference to an overriding theory or logic of understanding how the public interest concept relates to data protection. Thus, it is entirely unconvincing to argue that data controllers' or courts' interpretation of the public interest should be confined to this arbitrary list provided in the law.

Third and finally it can be said that in data protection the focus of the public interest conditions is on content; whereas in copyright it seems that the law is intended to focus upon the form of the work in question. The CDPA confers a negative right on the copyright holder; it does not provide the owner a positive right to publish their works. Rather, it prohibits others from publishing those works in the same *form* and does not generally prevent the publication of the ideas (the content) within that work. Given the focus on form underlying copyright law, there is no authority to assess the public interest in the *content* of a copyrighted work as this would be outside the purpose of the

[738] See Chapter 3 Sections 2.6.1.3 and 2.7.
[739] See Chapter 3 Section 2.6.

statute. The reason for this focus on form rather than content in copyright may be attributed to:

> an appreciation on the part of the legislature that it is unwise to spell out in too much detail what 'a work' will look like and from an understandable reluctance on the part of the judiciary to engage in consideration of the aesthetic merits of a work.[740]

Now let us reconsider the argument posed at the beginning of this chapter, that the public interest is not capable of precise definition and that it may be *counter* to the public interest to claim to have defined it in a final sense. If we consider the approach taken by Parliament to copyright, it is arguable that in the data protection context, they deliberately did not define the substantive content of the public interest in the conditions for processing under the DPA 1998. Just as Parliament was aware of its inability to predetermine the aesthetic content of a copyrightable work, there seemingly was also an awareness that they could not conclusively define the types of data processing which might serve the public interest. Both the aesthetics of a copyrightable work and the processing of data require normative judgments that are best left to fact-sensitive determinations in context.

Nevertheless, as opposed to the regulatory focus of the CDPA on the *form* of copyrighted works, the public interest determination required by Schedule 2, paragraph 5(d)[741] is *inherently* about *content*. To justify the processing of personal data on this condition, it must be substantively considered to be 'in the public interest'. It is impossible to exhaustively define all forms of data processing that are or would be considered in the public interest for the purposes of Schedule 2 of the DPA 1998 (or conditions under the DPPSPD 2000). Likewise, it is impossible to say that a public interest determination made at one point in time would be valid in the future. This is arguably why the public interest is *not* defined in the DPA 1998 or DPD. Thus, in the case of data protection (as opposed to copyright) the same valid (or persuasive) reasons to be confined to any predetermined understanding of the public interest are absent. Indeed, if we accept the theoretical conclusions reached in Chapter 4, there is *no* settled

---

[740] Burrell and Coleman (n 707) 103.
[741] Or indeed by the DPPSPD 2000, para 9.

and pre-determined understanding of the public interest in data protection that could be referred to on an ongoing and consistent basis as this would be *counter* to the essential contestability of the concept and its multiplicity (the need to cater for multiple public interests, including the protection of informational privacy and in certain uses of data).

3.1.4 The current state of the defence post-*Ashdown*

Only months after the decision in *Hyde Park II,* the Human Rights Act 1998 ('HRA 1998') came into force (on 2 October 2000) incorporating into UK law the rights contained within the ECHR.[742] The impact of this would be that once again the Court of Appeal would change tack and re-adjust the apparent scope of the public interest defence to give full effect to the HRA 1998 and in particular to Article 10 and the freedom of expression.

Ashdown v Telegraph Group Ltd ('*Ashdown I*') involved a claim for copyright infringement on the basis of publication of confidential memoranda belonging to the former leader of the Liberal Democrats, Mr Paddy Ashdown.[743] These memoranda detailed among other events, an important meeting after the general election in May 1997 regarding formal co-operation between Labour and the Liberal Democrats and for review of the voting system.[744] Ashdown publicly discussed his desire to publish these memoranda in a memoir. Before Ashdown could publish his memoirs, the *Sunday Telegraph* obtained a copy of the memoranda detailing Ashdown's meeting minutes from 21 October 1997 and published three stories on this basis. Ashdown lodged a claim for copyright infringement and succeeded, the Vice Chancellor ruling that the HRA 1998 did not extend the available defences for copyright infringement. [745] The *Sunday Telegraph* claimed that by section 171(3) of the CDPA the Court could give effect to the right to freedom of expression and in certain cases consider it to outweigh the interests of the copyright holder.

---

[742] Incorporated into Scottish law by the Scotland Act 1998 s 57(2) and in Northern Ireland by the Northern Ireland Act 1998 s 24(1).
[743] *Ashdown v Telegraph Group Ltd* [2001] EWHC Ch 28 ('*Ashdown I*').
[744] [2001] EMLR 44 [4]-[5] ('*Ashdown II*').
[745] *Ashdown I* (n 703) [15], [32].

The Court of Appeal in *Ashdown II* reversed the Vice Chancellor's ruling and reinstated the broader version of the public interest defence developed in *Lion Laboratories*. First, the Court held that:

> …rare circumstances can arise where the right of freedom of expression will come into conflict with the protection afforded by the Copyright Act, *notwithstanding the express exceptions to be found in the Act*. In these circumstances, we consider that the court is bound, insofar as it is able, to apply the Act in a manner that accommodates the right of freedom of expression.[746]

Second, and specifically as to the public interest defence, the Court found that

> Now that the Human Rights Act is in force, there is the clearest public interest in giving effect to the right of freedom of expression *in those rare cases* where this right trumps the rights conferred by the Copyright Act. In such circumstances, we consider that s 171(3) of the Act permits the defence of public interest to be raised.[747]

Similar to the remarks of Lord Justice Mance in *Hyde Park II*, the Court did not think it was possible to define the scope of the defence any further, beyond that it would only arise in very 'rare' circumstances.[748] Further clouding the discussion around the defence, the Court stated that 'quite apart from the ambit of the public interest defence under section 171(3)' the Court must always consider the potentially overriding public interest in the protection of human rights such as the freedom of expression. The impact of *Ashdown II* on the public interest defence is best described by Griffiths:

> …the Court of Appeal couched its decision in such dissuasive terms and refused so ostentatiously to prescribe a workable definition of the defence that it effectively killed it off again. As a result, contemporary commentators describe the defence with something approaching bemusement.[749]

The uncertainty surrounding the scope of the defence has since been exacerbated by the introduction of the Information Society Directive which does not permit Member States to retain exceptions to copyright in their domestic law that are not explicitly provided in the Directive.[750] Crucially, there are no exceptions in the Directive which

---

[746] *Ashdown II* (n 704) at [45] (emphasis added).
[747] ibid [58] (emphasis added).
[748] ibid [59].
[749] Griffiths (n 712) 83.
[750] Information Society Directive, Recital 32.

are clearly equivalent to the public interest defence in section 171(3) of the CDPA calling into question the validity of the defence in the UK. While some have argued that a more purposive reading of the Directive supports the application of the public interest defence in UK law,[751] it remains subject to considerable uncertainty in practice.[752] Nor has subsequent case law since *Ashdown II* clarified the scope of the defence. For example, in *HRH Prince of Wales v Associated Newspapers Ltd*, Mr Justice Blackburne held that the public interest defence did not apply because 'There is nothing in the material before me to indicate that this is or may be one of those rare cases where the public interest trumps the rights conferred by the 1988 Act.'[753]

In attempting to unpack the purpose and function of the public interest defence, Griffith persuasively argues that it is intended to act as a form of *pre-emption*:

> When pleaded successfully, the defence has functioned as a form of pre-emption doctrine, allowing the apparently binding rules of the CDPA, or its statutory predecessor, to give way before other, more compelling, legal norms.[754]

This is evident from the case law where the defence has been raised: in those cases, the Courts have been tasked with balancing the aims of copyright with the adjacent causes of action (mostly breach of confidence). On this analysis, the public interest defence in copyright law must be read as part of the wider legal schema that applies to information society and should be interpreted with a view to achieving external coherence with cognate areas of law. Commentators have considered whether a general 'freedom of expression' exception to copyright law might fare better at achieving this, although the precise contours of such a defence is far from certain; moreover, it could inevitably lead back to the same normative considerations required under the public interest defence – what is sufficiently in the public interest to justify the use of

---

751 Burrell and Coleman (n 707) 107–108; Kevin Garnett, 'The Impact of the Human Rights Act 1998 on UK Copyright Law', *Copyright and Free Speech: Comparative and International Analyses* (OUP 2005) 177–178.
752 Griffiths (n 712) 85–88.
753 [2006] EWHC 522 2008] Ch 57 [180].
754 Griffiths (n 712) 92.

copyrighted material?[755] From this bed of uncertainty what can be learned for the data protection context?

3.2 Generalisable and distinguishing features of the public interest in copyright

From examining the development of the public interest defence in copyright law, it appears that the defence will only succeed in rare cases 1) where a specific statutory exception does not apply and 2) that the 'routine' use of the defence would undermine the compromises made by Parliament to recognise certain discrete exceptions to the protection of copyright. The examination of the public interest at work in copyright, in this more narrow and uncertain scope, contrasts with and highlights the broader function and important role of the public interest conditions for processing personal data.

The public interest conditions are not failsafe 'exceptions' upon which data controllers may 'defend' their use of personal data. Rather, the conditions are one of several means by which they can legitimise their use of personal or sensitive personal data. It is important to distinguish between a defence or exemption on the one hand and a provision promoting or facilitating lawful action on the other as this difference in function already indicates a great deal about how the public interest should be deployed in either context. In the former case, as in copyright, a defence that is without clear definition such as under section 171(3) of the CDPA, should (and will) logically apply in more narrow circumstances. This can be contrasted to more defined action-promoting provisions, such as the public interest conditions under the DPA 1998.

To further support this distinction, consider that there is no explicit hierarchy between the conditions under Schedule 2 or 3 of the DPA 1998, and thus no risk of 'undermining' the efforts of Parliament if data controllers were to routinely rely upon the public interest conditions. To rely upon the public interest to justify the processing

[755] Yin Harn Lee, Emily Laidlaw and Daithí Mac Síthigh, 'Copyright and Freedom of Expression: A Literature Review' (2015) 206–210 <http://www.create.ac.uk/publications/copyright-and-freedom-of-expression-a-literature-review/>.

of personal data is *not* subverting an otherwise valid statutory route to processing; it is specifically in line with the relevant statute (negating such concerns as when applying the public interest defence in copyright).

The key lesson learned from copyright is that we must not leave the important task of clarifying the function and scope of the public interest conditions to the courts. While this may be understandable, if not appropriate, to the application of the narrow public interest defence in copyright, the action promoting and integral role played by the public interest conditions requires significantly more attention if the conditions are to be deployed consistently with the aims of data protection law. Amended legislation and authoritative guidance can more successfully guide the application of the public interest conditions, as evidenced by the implementation of the public interest concept in freedom of information law.

4. Public Interest Disclosures under Whistleblowing Law

Whistleblowing refers to '…the disclosure by organization members (former or current) of illegal, immoral or illegitimate practices under the control of their employers, to persons or organizations that may be able to effect action.'[756] In the UK, whistleblowing is another area of law where the public interest concept is used without being plagued by ambiguity. Under the UK's Employment Rights Act 1996 ('ERA'), as amended by the Public Interest Disclosure Act 1998 ('PIDA'), whistleblowers are protected if their disclosures are in the public interest.[757] Until June 2013[758], the term the 'public interest' was not explicitly used within the ERA or PIDA; its use was limited to the title and introductory text of the PIDA. This prefacing material is nonetheless instructive as to the concept's intended role within the legislation: 'An Act to protect individuals who make certain disclosures of information in the public interest; to allow

[756] Marcia P Miceli and Janet P Near, *Blowing the Whistle: The Organizational and Legal Implications for Companies and Employees* (Lexington Books 1992) 15.
[757] The Employment Rights Act 1996 ('ERA'); The Public Interest Disclosure Act 1998 ('PIDA').
[758] ERRA, s 17. In 2013, the Enterprise and Regulatory Reform Act ('ERRA') amended the ERA. To qualify as a protected disclosure, individuals would now have to reasonably believe their disclosure was 'in the public interest'. I will discuss this point further below.

such individuals to bring action in respect of victimisation; and for connected purposes.'[759]

4.1 The meaning of the public interest in whistleblowing law

The public interest in whistleblowing is in part encapsulated by the subject matter of disclosures that qualify for protection, listed under section 43(b) of the ERA. 'Qualifying' disclosures *must* relate to one of the six specific types of 'relevant failures' by the employer organisation:

> (a) that a criminal offence has been committed, is being committed or is likely to be committed,
> (b)that a person has failed, is failing or is likely to fail to comply with any legal obligation to which he is subject,[760]
> (c)that a miscarriage of justice has occurred, is occurring or is likely to occur,
> (d)that the health or safety of any individual has been, is being or is likely to be endangered,
> (e)that the environment has been, is being or is likely to be damaged, or
> (f)that information tending to show any matter falling within any one of the preceding paragraphs has been, is being or is likely to be deliberately concealed.[761]

Thus, in whistleblowing, public interest disclosures are confined to a subset of factual circumstances. To be 'in the public interest' and qualify for protection under the ERA, the disclosure must implicate the subject matter provided in section 43(b). This is clearly in contrast to data protection where the meaning of the public interest has been left open to interpretation and moreover, the subject-matter of processing that may be justifiable in the public interest is impossible to define in a similarly exhaustive sense. This is not least because of the constantly growing range of data processing possibilities which may serve the public interest in uniquely innovative ways.

In reviewing this list of qualifying disclosures, we can understand the meaning of the public interest concept in whistleblowing. Here it seems that the 'public interest' is used to prevent, shed light on, rectify or mitigate apparent harms to societal interests. In

---

[759] PIDA, Introductory text.
[760] *Parkins v Sodexho Ltd* [2002] IRLR 109 (EAT). After *Parkins*, Section 43(b) was considered to include disclosures regarding the breach of the individual employee's own contract with the defendant employer organisation.
[761] ERA, s 43(b), as inserted by PIDA, s 1.

other words: 'It is in the public interest that negligence in the workplace be eliminated, health and safety violations be corrected, and criminal wrongdoing be exposed and prosecuted.'[762] Concomitantly, the 'public interest' in whistleblowing is also clearly about protecting the individuals who make disclosures regarding such matters.[763] Although not made explicit in the introductory text of the PIDA, employee-employer confidentiality is also a public interest that is valued and protected within the legislation.

On confidentiality, under section 43(G)(3)(d) of the ERA, the reasonableness of an individual's disclosure will be assessed as to '…whether the disclosure is made in breach of a duty of confidentiality owed by the employer to any other person'.[764] Protection for whistleblowers is more easily secured when disclosures are made *internally* to employers, seen by the stricter requirements imposed for protection of *external* disclosures to third parties. Therefore, the public interest in maintaining confidentiality between an employee and his/her employer is prioritised over the public interest in disclosure: '[whistleblowing] is perceived as a justified breach of confidentiality; hence, intra-organizational disclosure is required, because it permits correction of the problem without confidentiality being breached.'[765] In summary, whistleblowing legislation attempts to:

> …strike an intricate balance between (a) promoting the public interest in the detection, exposure and elimination of misconduct, malpractice and potential dangers by those likely to have early knowledge of them, and (b) protecting the respective interests of employers and employees. There are obvious tensions, private and public, between the legitimate interest in the confidentiality of the employer's affairs and in the exposure of wrong.[766]

---

[762] James Gobert and Maurice Punch, 'Whistleblowers, the Public Interest, and the Public Interest Disclosure Act 1998' (2000) 63 The Modern Law Review 25, 38 (emphasis added).
[763] Consider the introductory text to PIDA: 'An Act to *protect individuals* who make certain disclosures of information in the public interest; *to allow such individuals to bring action in respect of victimisation*; and for connected purposes' (emphasis added).
[764] ERA, s 43(G)(3)(d), as inserted by PIDA, s 1.
[765] Elletta Sangrey Callahan, Terry Morehead Dworkin and David Lewis, 'Whistleblowing: Australian, U.K., and U.S. Approaches to Disclosure in the Public Interest' Virginia Journal of International Law 879, 899 (emphasis added).
[766] *ALM Medical Services Ltd v Bladon* [2002] EWCA Civ 1085, [2002] Emp LR 1054 [2].

4.2 The remedial role of the public interest in whistleblowing

It may seem that it is the role of whistleblower protections to promote a particular public interest i.e. in whistleblowing. However, the legislation has been primarily motivated by its desired remedial effects; as provided by Callahan et al:

> …the discussion of the U.K. legislation emphasized ending 'the "culture of fear" among workers who are afraid to reveal wrongdoing,' but did not mention promoting whistleblowing. Thus, at least publicly, the statute was presented as a remedial measure.[767]

In support of this view, consider that the legislation imposes no *positive* duties on employers to promote whistleblowing or otherwise support it within their organisations: '…while PIDA may protect whistle-blowers from reprisals, it does not obligate an employer to give credence to or do anything about a whistle-blower's charges.'[768] Indeed, 'The Act itself neither encourages nor discourages whistleblowing except indirectly.'[769] Rather the legislation focuses on deterring organisations from any retaliatory action if protected disclosures are made by their employees.[770] How does this contrast with the public interest conditions?

Under the DPA 1998 the public interest conditions are there to *facilitate or further* a particular public interest served by lawful data processing. Thus, in contrast to the *ameliorative* and *protective* role of the public interest in whistleblowing, the concept is used in data protection to *promote* certain forms of processing that are perceived as publicly beneficial.[771]

---

[767] Callahan, Dworkin and Lewis (n 765) 884.
[768] Gobert and Punch (n 762) 38.
[769] ibid (emphasis added).
[770] In specific sectors, whistleblowing may be more explicitly promoted in future. Consider the recent changes to whistleblowing policies in the financial sector, promulgated by the Financial Conduct Authority and Prudential Regulation Authority. As of 7 March 2016, large financial institutions (e.g. deposit takers with more than £250 million in assets) must have appointed 'whistleblowing champions' who have '…the responsibility for ensuring and overseeing the integrity, independence and effectiveness of the firm' s policies and procedures on whistleblowing'. These new rules seem to more explicitly promote whistleblowing than in the more generally applicable ERA. Financial Conduct Authority, 'Accountability and Whistleblowing Instrument 2015' s 18.4.4 <https://www.handbook.fca.org.uk/instrument/2015/FCA_2015_46.pdf>.
[771] Similar distinctions can be made, for example, between the role of the public interest in whistleblowing as preventative and that in publicity cases. Black argues that 'Where use of persona is necessary to communicate cultural meaning, as advanced by Madow, Coombe, Carty and de Grandpre, amongst others, then it should be permitted, on the basis of the public interest in allowing such use. Whereas the public interest is typically cited in the context of criminal behaviour or iniquity or public

A further distinction should be made here as to the public interest in confidentiality protected within the ERA, whereby whistleblowing will almost always violate confidentiality between an employee and his/her employer. This contrasts with data protection law because the use of personal data is *not* a violation, per se, of an individual's rights and interests in his/her data. The DPA 1998 does not consider individuals' rights and interests as automatically compromised merely because their personal data are processed based on the public interest conditions as opposed to consent or some other justification. Moreover, the conceptualisation of the public interest put forward in this thesis is that a public interest use of personal data can also be directly or indirectly in the interests of an individual, as a member of the relevant public.

4.3 The procedure for assessing the public interest in whistleblowing

To be 'protected' a whistleblower's disclosure must pertain to the subject matter referred to in section 43(b) of the ERA (as provided above). The disclosure must also conform to a variety of other requirements:

- The individual must actually *make* the disclosure;[772]
- The individual must have a *reasonable belief* that their disclosure 'tends to show' the occurrence (or likely occurrence) of one of the relevant failures in section 43(b) of the ERA;[773]
- The individual must have a *reasonable belief* that their disclosure '*is in the public interest*';[774]

protection, this alternative ground would see it employed in a more creative and positive context.' Gillian Black, 'A Right of Publicity in Scots Law' (University of Edinburgh 2009) 247–248 <https://www.era.lib.ed.ac.uk/bitstream/handle/1842/5943/Black2009.pdf?sequence=1>.

[772] The disclosure must convey facts, not merely make an allegation or state the position of the whistleblower. *Cavendish Munro Professional Risks Management Ltd v Geduld* [2010] IRLR 38 (EAT) [24]-[26].

[773] Whereby the whistleblower's belief must be 'objectively reasonable' even if it turns out to be wrong. *Babula v Waltham Forest College* [2007] EWCA Civ 174 [75], [79].

[774] The requirement that disclosures were to be made in 'good faith' was repealed in the ERRA, s 18 and replaced with this requirement to reverse *Parkins* (n 760). As provided in subsequent case law, reviewing the meaning of the 'public interest', Mr Justice Supperstone reminded the parties that 'The words "in the public interest" were introduced to do no more than prevent a worker from relying upon a breach of his own contract of employment where the breach is of a personal nature and there are no wider public interest implications.' *Chesterton Global Ltd (t/a Chestertons) and another v Nurmohamed* [2015] UKEAT [36].

- The individual must abide by the requirements when disclosing to particular parties (i.e. to the employer '*internally*' or to a third party '*externally*')[775].

As stated above, until 2013 there was no explicit use of the term 'public interest' in the ERA. However, in response to the ruling in *Parkins v Sodexho Ltd.*[776], which provided that a qualifying disclosure could encompass the breach of an *individual* employee's employment contract, the ERRA created a public interest requirement for disclosures. Section 18 of the ERRA repealed the requirement that disclosures had to be made in 'good faith'[777], and replaced this with section 17 which requires disclosures to be made in the *reasonable belief* that it is in the public interest.[778] This effectively created a 'public interest' test to determine whether a disclosure would qualify for protection.

In subsequent case law interpreting this requirement, the Employment Appeals Tribunal ('EAT') found that a disclosure regarding a potential wrongdoing impacting upon '100 senior managers' was sufficiently 'in the public interest'.[779] It did not matter that the claimant was primarily concerned with the effect on himself or that the employer was a private sector firm as opposed to a public authority.[780] Importantly, the EAT stated that it was not its duty to consider whether the disclosure was in fact 'in the public interest' but rather that the claimant reasonably believed it was.[781] The standard for reasonable belief remained the same as provided for in *Babula*[782] and thus:

> …the public interest test can be satisfied where the basis of the public interest disclosure is wrong and/or there was no public interest in the disclosure being made provided that the worker's belief that the disclosure was made in the public interest was objectively reasonable.[783]

---

[775] Disclosure to employers (internally) is promoted within the ERA. There are significantly more requirements for disclosures to be protected if the disclosure is made to third parties; particularly strict rules are in place for disclosures to the media. ERA, s 43(c)-43(h).
[776] *Parkins* (n 760).
[777] Previously, ERA, s 43(c)(1).
[778] ERRA, s 17-18.
[779] The claimant's disclosure was regarding the alleged manipulation of accounts by his employer, with potential adverse effect on the bonuses of 100 senior managers including himself: *Chesterton* (n 774) [38].
[780] *Chesterton* (n 774) [38]-[39].
[781] ibid [28].
[782] *Babula* (n 773) [75].
[783] *Chesterton* (n 774) [34].

When contrasting the public interest test in whistleblowing with the public interest conditions in data protection, we see the importance of *procedural* principles that can be applied across different factual circumstances in a consistent manner. Here there are at least broad similarities between the procedural requirements for 1) relying upon the public interest to protect disclosures and 2) justifying the processing of personal data based on the public interest. However, in data protection there lacks a specific procedure or standard for reviewing a data controller's reliance on the public interest conditions. The result of this is a lack of consistency in how data controllers, regulators and courts will assess the public interest in data processing. How can this consistency be achieved?

It is arguable that the more that guidance is provided, within the legislation itself or in subsequent cases and regulatory guidance, decision-makers are at least *more capable* of taking a consistent approach to assessing matters of the public interest. For example, in freedom of information law, both the ICO and SIC have provided clear guidance in extrapolating guiding principles from specific examples of where the public interest in maintaining an exemption would outweigh the public interest in disclosure. Both the ICO's and SIC's guidance allows public authorities to engage more consistently with the public interest test. This contrasts with the copyright context where neither the CDPA nor subsequent case law has provided guiding principles or clear examples of the range of 'rare' circumstances in which the public interest test might be applicable. Considering the narrower role of the public interest defence, the courts take a far more active approach to interpreting the circumstances in which the public interest defence applies in copyright.

As argued throughout this thesis, the public interest is an inherently context-sensitive concept. Thus, contextual analysis will be required whenever the concept is deployed. Nevertheless, it is possible and indeed necessary to draw from specific cases, guiding principles for applying the public interest to a context where it plays an action promoting role as it does in the public interest conditions in data protection. This level of guidance is required if decision makers are to avoid the conceptual vulnerabilities of the concept highlighted in Chapter 4 and thus achieve any form of consistency when applying the public interest in a legal context.

Would introducing a standard of reasonable belief as exists under whistleblowing law add any certainty and consistency to the application of the public interest conditions in data protection? Using the mixed test of reasonable belief under whistleblowing law as a potential model for assessing public interest considerations,[784] the *reasonableness* of a data controller relying on the public interest in their data processing would be assessed from an *objective* standpoint but their *belief* would be assessed *subjectively*. There are at least three distinctions to make between whistleblowing and data protection which may explain 1) why such a standard was not introduced in the public interest conditions and 2) why it is difficult to anticipate what standard *would* apply. These distinctions centre around the focus in data protection on the substantive content of the public interest claim, the lack of any standard, and lack of any requirement, to assess a data controller's reliance on the public interest conditions.

First, in whistleblowing, the focus is on the whistleblower and the reasonableness of their belief that their disclosure is in the public interest, as opposed to the focus in data protection's public interest conditions on the substantive and normative *content* of the 'public interest' claim. In data protection, the focus is on the nature of processing in question – whether that processing is necessary for a function 'of a public nature' and is *in* the public interest. The focus is *not* on the data controller and how reasonable their beliefs are that any of these requirements have been met. Thus, in data protection, data controllers and courts must directly engage with the *substance* of the question – is this processing in the public interest? – a question which is explicitly avoided in whistleblowing law.[785]

---

[784] In reference to the standard of 'reasonable belief' under the ERA where 'the word belief is subjective but the reasonableness of it is to be determined objectively.' This can be understood as a 'mixed' test of reasonable belief, as in general legal understandings an 'objective' test of reasonable belief requires the fact finder to assess the relevant facts from the viewpoint of the hypothetical reasonable man/woman. In contrast, a purely 'subjective' test would assess the circumstances taking into account the particular characteristics of the person/persons in question. A 'mixed test', as used in whistleblowing, combines these elements (e.g. 'reasonable belief' with reasonableness assessed from an objective standpoint but belief from a subjective one). David Lewis, 'Ten Years of Public Interest Disclosure Legislation in the UK: Are Whistleblowers Adequately Protected?' (2008) 82 Journal of Business Ethics 497, 499.
[785] As provided in *Chesterton* (n 774) [28].

Second, and relatedly, unlike the requirements for protected disclosures under the ERA, there is no explicit standard for evaluating a data controller's reliance on the public interest conditions. Compared to the freedom of information context, the ICO has remained silent on what approach they might take to evaluating data controllers' claims that their processing is justified based on the public interest conditions.[786]

A third distinguishing characteristic of the public interest in whistleblowing is the fact that whistleblowing claims will often revolve around the veracity of the employee's disclosure versus the employer's own defensive assertions, thus requiring a clear standard upon which to evaluate those competing claims. Employees' (the whistleblowers') disclosures are scrutinised as to the facts conveyed; the reasonable belief and public interest in the disclosure and in terms of who the disclosure was made to. In data protection, there are currently no requirements for data controllers to account for or otherwise substantiate their reliance on a condition for processing (although it may be prudent to do so). As such, the 'legitimacy' of a data controller's reliance on the public interest is not as explicitly scrutinised as are the claims of a whistleblower. It is worth bearing in mind, again, the guidance on the public interest test in the freedom of information context where the Information Commissioner advises public authorities to identify the public interest arguments on both sides and document this.[787] It is reasonable to assume that whatever approach is taken by the ICO when assessing data controllers' reliance on the public interest conditions, that it would be beneficial for data controllers to produce documentation that demonstrates their consideration of the issues. I raise this point specifically in my suggestions for amending the public interest conditions in Chapter 6.

In data protection, the principle of proportionality is likely to be key to evaluating a data controller's reliance on the public interest conditions. If the data processing in question was proven to not be particularly risky or harmful to the relevant publics and

[786] While this is not precedent setting for, or directly applicable to interpreting the public interest conditions, I consider the application of a reasonable belief standard to s 32 of the DPA 1998 when I suggest a mixed test of reasonable belief should be introduced as an amendment to the public interest conditions. See Chapter 6 Section 3.2.
[787] ICO, 'The Public Interest Test: Freedom of Information Act' (n 651) 9.

individuals in question, and a data controller could demonstrate that they have thought through such considerations, then a potentially more forgiving standard would apply. Such a standard could take into consideration the *subjective*, albeit objectively reasonable, belief of the data controller that the processing was necessary in the public interest.[788] This remains pure speculation until such a case arises in the context of the public interest conditions.

4.4 Generalisable and distinguishing features of the public interest in whistleblowing

There are clear distinctions in substance, purpose and procedure between the public interest in whistleblowing and in data protection law. In whistleblowing, the substantive meaning of the public interest is more tightly confined to a set of factual circumstances provided in the legislation as opposed to the non-exhaustive list of examples of public interest uses of data provided in data protection law. Where the public interest plays a more corrective and defensive role in whistleblowing, in data protection it takes on a more positive, action supporting role, promoting publicly beneficial forms of processing personal data. Although in both areas of law reliance on the public interest is conditioned on the satisfaction of particular procedures, the focus is materially different. In whistleblowing, the focus is on the claimant: is their claim to the public interest reasonable? Whereas with regards to the public interest conditions, the focus is on the substance of the claim: is the processing substantively in the public interest? It is possible that the lack of an approved standard for evaluating a data controller's claim, that a type of processing is 'in the public interest', has been a source of discomfort and uncertainty for data controllers. In the following chapter, I will explore the need for and viability of introducing a standard of review to evaluate claims that the processing of personal data is justified in the public interest.

[788] See note 784.

5. Conclusion: Common and Context Specific Features of the Public Interest Concept

In examining the use of the public interest across freedom of information law, copyright and whistleblowing, certain features of the public interest are *generalisable* and *applicable* to understanding and deploying the concept in data protection.

First, from **freedom of information law**, we see that the provision of descriptive examples is helpful to guide the discretionary and context-sensitive nature of public interest determinations. Providing examples where the public interest threshold would be met but also examples where the threshold would *not* be met can provide substance to the inherent ambiguity of the concept. Furthermore, although the concept must be assessed in context, there are likely to be key principles that can be extracted from particular factual circumstances where the public interest is deployed. These can be used to focus decision-makers on relevant criteria to consider when applying the public interest to their own circumstances, while alerting them to factors which are irrelevant and should not play a role in such considerations. The point being, even if bright line rules are impossible to give in any context where the public interest concept is deployed, it *is* possible to provide legal clarity on the range of plausible applications in a particular context. Comprehensive guidance, including relevant, practical examples and guiding principles, is even more critical where individual decision-makers are tasked with independently making public interest determinations in the first instance.

Second, from the uncertainty surrounding the role and status of the public interest defence **in copyright**, we see the importance of understanding the role and scope of public interest within legislation and how this should dictate the level of guidance provided. If the public interest is operating as an *exemption* or *defence* in law, this lends to narrower boundaries of application. Where the public interest plays this more limited role, it may be more appropriate for the courts to determine the circumstances where such an exemption or defence applies. In contrast, where the public interest is intended to function in a more action-promoting and positive role within the law, this requires substantially different legal intervention. The latter case, which applies to the public interest conditions in data protection, necessitates authoritative guidance (as

opposed to ad hoc judicial interpretations) to provide the detail necessary for the public interest to be deployed in these broader circumstances.

Third, from the **whistleblowing** context, we see the importance of individual decision-makers knowing in advance how their claims of the public interest will be evaluated by regulators and courts. Are their claims evaluated based on what was subjectively reasonable to them, will a stricter objective standard apply or a mix of the two as is the case in whistleblowing? At what point is the public interest threshold met in a particular, legal context? The lack of an approved standard for evaluating a data controller's claim that a particular type of processing is 'in the public interest' has been a source of uncertainty, a point which I will return to in the following chapter.

The table on the following page summarises the three areas of law considered in this chapter as compared with the parameters of data protection law as they currently stand. It is the cumulative legal and theoretical analysis undertaken in Chapters 3, 4 and 5 that allows me to formulate a new understanding of the public interest concept in data protection and to propose new procedures for deploying the public interest conditions in Chapter 6.

Table 4

	Data Protection Law	**Freedom of Information Law**	**Copyright Law**	**Whistleblowing Law**
What role does the public interest play?	Action-promoting provision.	Exemption to disclosure.	Fail-safe defence when other more specific exceptions do not apply.	Last point in consideration for legitimising the protection of a whistleblower's disclosure.
Is the public interest defined?	No, but indirectly the DPD sets forth the protective *and* facilitative aims of implementing legislation. Thus, there are *two* general public interests at stake: the protection of individuals' informational privacy and in certain uses of data (subject to	Disclosure is prioritised over specifically defined public interests where an exemption to disclosure may apply.	No, but recent case law indicates a trend towards interpreting the public interest defence in terms of protecting the freedom of expression. Previous cases indicate that the	No, but the public interest is 1) confined to a set of factual circumstances surrounding disclosures and 2) is focused on balancing the public interest in disclosure versus the public interest in protecting

	relevant conditions being met).		public interest refers to avoiding wrongdoing by *not* enforcing copyright in particular circumstances.	employer/employee confidentiality.
Is there a set procedure or standard for assessing the public interest?	Currently, there are no principles or legal precedent to guide application of the public interest conditions.	The public interest test is routinely applied and subject to comprehensive guidance providing principles and specific examples of how the public interest has been deployed.	The defence is applied on a case-by-case basis by the Courts, given the narrow role assigned to the defence in the legislation.	Whistleblower claims are evaluated according to the standard in *Babula*: a whistleblower must prove they made their disclosure in the reasonable belief that it was in the public interest to do so.

Chapter 6 Key Components and a New Approach to Making Public Interest Determinations in Data Protection Law

1. Introduction

Data protection law uses the public interest concept at critical legal junctures without providing a means to deploy it consistently with either the public interest in protecting informational privacy or in certain publicly beneficial uses of data. As discussed in Chapter 2, the predominant means of compliance with data protection law, through consent or anonymisation, is unable to account for, in any meaningful way, the full spectrum of rights and interests at stake in any given data processing situation. Indeed it hinders both the protection of informational privacy and the undertaking of publicly beneficial forms of research. The extensive legal analysis in Chapters 3 and 4 exposed conceptual gaps in understanding what the public interest means in data protection. This lack of a fuller public interest concept has hindered its deployment in the public interest conditions for processing. The theoretical analysis in Chapter 4 provided insight on the conceptual boundaries of the public interest and highlighted relevant and non-relevant factors for deciding on matters of the public interest in a normative sense.

To further test this developing understanding of the public interest as a concept, and to broaden the legal evidence base, I examined the use of the public interest in cognate areas of law. Analysis of the public interest test in freedom of information, the public interest defence in copyright and the public interest test in whistleblowing emphasised what should be done and what should be avoided if we are to develop a more objective and consistent approach to the public interest conditions in data protection.

Based on this legal and theoretical analysis, in this chapter I set forth the key components of a proposed new approach to understanding the public interest concept

in data protection and a series of suggested changes to the law and related procedures for making public interest determinations. The conceptual insights offered and the practical changes suggested present a framework for making public interest determinations in data protection law where there currently is none, and for actively and more openly considering the multiple public interests at stake.

This chapter begins with a review of the key vulnerabilities of the public interest concept (discussed in Chapter 4) which any theory on the public interest must avoid. Following this I suggest four key components which should be used to assess the public interest in processing and cumulatively represent a new understanding of the public interest concept in data protection. I translate this into a public interest 'checklist' for data controllers, which highlights the key questions they must answer when assessing the public interest in their processing. This format was devised based on the guidance provided by the ICO and SIC (discussed in Chapter 5), which successfully enables public authorities to apply the public interest test in the freedom of information context.

The remainder of the chapter focuses on establishing for the first time a robust procedure for making public interest determinations in UK data protection law. My approach builds upon the current law, fills the conceptual gaps identified in Chapter 4 and takes heed of the lessons learned from freedom of information, copyright and whistleblowing legislation in Chapter 5. I suggest both legislative changes and two alternative procedures for deploying the new understanding of the public interest concept presented. I propose changes to the existing public interest conditions to explicitly recognise the public interest (in addition to the private interest) in the protection of informational privacy. I further suggest how public interest determinations can be made more transparently, and consistently, by introducing a mixed test of reasonable belief for assessing a data controller's reliance on the public interest conditions.

The suggested procedural changes are drawn from both the legislation examined in Chapter 5 as well as currently working solutions in analogous legal contexts, notably in

Australia, where legislation and authoritative guidance make clear how and when public interest determinations are made within the scope of federal privacy law. The chapter concludes by explaining the key differences between the conceptual and practical approach developed in this thesis and the status quo, and therefore how my contribution improves and progresses current understandings of the public interest in data protection.

2. Vulnerabilities of the public interest

As discussed in Chapter 4, the public interest concept is inherently difficult to deploy in decision making and particularly in legal settings as it is an *essentially contested concept*.[789] The public interest cannot be defined in any conclusive sense and the ambiguity of the term makes it easy to exploit by those in power.[790] In any legal setting, not only in data protection, the deployment of the public interest concept can become 'questionable' especially where decisions justified on the basis of the public interest are made in *private* and are not subject to public scrutiny.[791] The opacity of such decision-making is not only problematic from an individual rights perspective. Where obtaining consent or anonymising data are not possible, and despite the potential public interest served by processing, data controllers lack the confidence to take decisions based on the public interest conditions given the absence of an accepted approach to do so under data protection law. In this scenario, publicly beneficial processing may not occur or the paradigm of consent or anonymisation is perpetuated to the detriment of individuals, data controllers and wider society.[792]

Below I will review the theoretical problems which plague the deployment of the public interest concept to reveal more clearly the vulnerabilities I seek to avoid in the key components to the public interest I propose in Section 3.

---

[789] See Chapter 4 Section 2. Gallie (n 49) 168–169.
[790] Mansbridge (n 49) 4–5.
[791] Flathman (n 573) 527–531; Mansbridge (n 49) 5.
[792] As discussed in Chapter 2.

2.1 Beyond empiricism

Utilitarian conceptions of the public interest equate the concept with that which benefits the majority. Thus, the public interest lies in the decision which delivers the greatest good to the greatest number of people. Termed 'preponderance theories' in Held's typology, these understandings of the public interest favour the majority interest despite any possibility that the 'good' delivered to the majority is minor if compared to the disproportionate, negative harm caused to a smaller number of people. Sorauf labels such theories as nothing more than counting noses,[793] meaning that this conception can only ever indicate what the majority opinion is. As discussed in Chapter 4, the public interest is *distinct* from the majority opinion, or in decision-making terms, is different from what is good for the greatest number. What is missing from preponderance theories is a way to jump from the empirical fact that 'x' course of action serves 'y' number of people to 'x' course of action is *normatively* in the public interest, which is the role assigned to the public interest in the data protection context.

Furthermore, if favouring majority interests, over all other interests, this neglects the values and protections embedded within data protection law including the overarching scheme of human rights legislation applicable to data processing. Preponderance theories do not provide sufficient weight and consideration of compelling minority interests which may outweigh the majority interest. The danger here, as described by Townend, is that:

> [If] one operates with the balance of the individual against the mass, the inevitable imbalance in favour of the majority can immediately be understood: a substantial damage to the particular individual is soon outweighed by the sum of the individually negligible benefits to the other individuals within the collective.[794]

In data protection, to move beyond current and ineffective approaches to compliance where the public interest in privacy is neglected and treated as a mere private interest, it is critical that any new theory of the public interest can identify cases where protecting individuals' informational privacy outweighs the benefits of a given form of

[793] Sorauf (n 56) 625.
[794] Townend (n 28) 99 See also: Stavros Tsakyrakis, 'Proportionality: An Assault on Human Rights?' [2009] International Journal of Constitutional Law 471.

processing, even if more people stand to benefit from the processing than would be harmed from it.

What role *does* public opinion play in determining which course of action serves the public interest? Is 'the public' not the best source of knowledge on what is in 'their' best interest? As Held asserted, the majority interest may well be one of many reasons to believe that 'x' course of action is in the public interest. [795] However, the deployment of the public interest in any given context means that '… we want to know something *else* than the empirical fact that it is in the interests of a preponderance of individuals.'[796] The public interest cannot be verified by empirical fact because empirical facts do not answer *why* 'x' is or is not normatively in the public interest.[797]

Nevertheless, meaningful public engagement is crucial to any reliance on the public interest to justify the processing of personal data. As evidenced by the care.data debacle in England discussed in Chapter 2, data controllers are simply not doing enough *meaningful* public engagement to support their reliance on the public interest to justify the processing of personal data. As Taylor argues in context with genetic data, it is not at all clear that the law accurately reflects and or understands the expectations of individuals as to certain uses of their data; this calls into question the legitimacy of any reliance on the public interest to justify such uses.[798] The results of meaningful public engagement can provide data controllers with a more informed and justifiable basis for relying upon the public interest for a given form of processing. Even if public engagement exercises cannot conclusively settle the conflicts of interests between those for or against a use of data, it *can* 'minimize the element of whim and caprice' and accusations of arbitrariness, when relying upon the public interest in decision-making.[799] Certainly, data controllers will be in a better position to make a decision regarding the public interest *after* engaging in public dialogue than before it.[800]

---

[795] Held, *The Public Interest and Individual Interests* (n 58) 84.
[796] ibid.
[797] As also argued by: ibid.
[798] Taylor (n 28) 34.
[799] Flathman (n 573) 531.
[800] ibid.

In summary, at least three important lessons emerge from my analysis, and ultimately my rejection of, preponderance theories:

- **The need to identify cases where the protection of informational privacy outweighs the need to pursue a public interest use of data;**
- **The need to distinguish between an empirical tabulation of individual preferences and the public interest in a normative sense;**
- **The value in facilitating public dialogue on data processing initiatives justified on the public interest.**

These lessons play important roles in my key components of the concept and proposed legislative solutions in Sections 3 and 4 below.

2.2 The impossibility of unanimity

Under common interest theories, the public interest is equated to what is in the interests of *all* individuals, at least in the long run. It is difficult if not impossible to imagine any interest that is truly unanimously shared amongst all individuals, or a procedure which could accurately tabulate this. Some have tried to compensate for this by theorising on the potential for 'net' common interests, where on balance, an interest can be said to be in everyone's interest. Under such theories, individuals are understood to play various roles in society, as a mother, father, employer, employee, and so forth. The one role *everyone* plays is the role as a member of the public. In this role individuals 'will naturally tend to favour goods or policies that are in the interest of everyone in society, rather than goods or policies that benefit us in some more particular role.'[801]

What is problematic with common interest theories is that the public interest is conceived as something that can be defined *conclusively*, once all the 'pluses' and 'minuses' of individuals' interests are balanced. In data protection legislation, the examples of public interest processing, (e.g. for research), were not included because they would *always* be in the public interest. For example, as discussed by Beyleveld, '…not all medical research is well-designed and constructed. Some of it might be very speculative, even fanciful, and some of it might be directed to ignoble ends and involve

[801] O'Flynn (n 49) 305 Similarly: Brian Barry, '32. Public and Common Interests' in Richard E Flathman (ed), *Concepts in Social and Political Philosophy* (Macmillan Publishing Co, Inc 1973).

means that are very serious violations of human rights.'[802] In such circumstances, clearly the research would *not* be justifiable in the public interest, even if medical research is recognised in data protection legislation as an example of processing that *may* be justifiable in the public interest.

Therefore, like preponderance theories, common interest theories do not allow for the identification of cases where individuals' interests and rights may outweigh the public interest in processing. Under common interest theories the public interest would become 'absolute' once the balancing is undertaken (or unanimity is found). Even if we accept that individuals play different roles in society, including as a member of the public, and that these roles translate to different types of interests, this does *not* mean the public interest can be defined conclusively by reference to this commonly held role. Instead, what can be taken from this analysis is the importance of context when determining precisely *who* will be impacted by a decision and thus which interests should be accounted for in any decision-making process.

Thus, the key lessons learned from my exploration and rejection of common interest theories include:

- **The need for a public interest concept to account for the *full* spectrum of interests at stake, regardless of how commonly or uncommonly held they are;**
- **The importance of context for assessing what the relevant interests are for a particular decision.**

As proposed in my key components in Section 3 below, the public interest is capable of *multiple* meanings which change over time and require contextual based assessments.

2.2.1 Beyond proceduralism

Within Chapter 4 I briefly considered an offshoot of common-interest theories which focus on the procedure involved in determining the public interest. Under such theories, the public interest only becomes meaningful in terms of the operation of

[802] Beyleveld (n 28) 287.

decision-making procedures.[803] According to such theories, the public interest *is* the outcome of an agreed upon procedure. However, just as the public interest is *more than* mere empirical facts, it is also more than procedure. Taylor argues that if decisions based on the common interest are to be *legitimate*, the decision-making processes must be transparent and justifiably account for the displacement of one interest over another.[804] A new approach to the public interest in data protection must indeed be capable of *legitimately* determining whether reliance on the public interest is appropriate in a processing context. Where currently no procedure exists for transparently determining whether a given form of processing is justifiable on the public interest conditions, in Sections 4 and 5 I suggest how data protection legislation should be amended to introduce such a procedure for the benefit of both data subjects and data controllers.

2.3 Beware of philosopher kings

The final theory of the public interest examined (and ultimately rejected), was unitary theories which define the public interest by reference to an absolute system of values that guide individual actions, even if individuals are unaware of it.[805] Individuals hold no place within this theory as neither the majority consensus nor any minority conflicting interest can impact what is in the public interest, as it is understood in an absolute sense. As argued in Chapter 4, in the data protection context, there are no 'philosopher-kings' who have the authority to determine conclusively what processing is justifiable in the public interest. Indeed, as argued above, the approach developed in this thesis rejects the idea that the public interest is representative of anything in a final or absolute sense. Data protection law simply does not provide fixed distinctions between what is and is not considered to be justifiable in the public interest. This would be counter to the primary aims of data protection law which recognises *both* the public interest in the protection of informational privacy and in *some* uses of data, the latter being subject to meeting the applicable legal standards.

---

[803] Buchanan and Tullock (n 589) 285.
[804] Taylor (n 28) 31.
[805] Held, *The Public Interest and Individual Interests* (n 58) 135.

Along similar lines to my rejection of common interest theories, no use of data will *always* be justifiable in the public interest in a final sense (which unitary theories demand). Nor is deciding that a type of processing *is* justifiable in the public interest an indication that informational privacy is not also a public interest. Any theory that does not recognise the prospect of *multiple* public interests existing within a context, makes reliance on the concept more susceptible to misuse by those who claim to have 'the authority to make such determinations.

Thus the crucial lesson learned from unitary theories of the concept is:

- **That we must recognise the prospect of valid yet conflicting public interests: the public interest in a use of data and in protecting individuals informational privacy may conflict but are both valid public interest claims in data protection.**

The key components of the public interest and legislative changes I propose in Sections 3-4 allows for legitimate conflicts between concurrently held public interests rejecting the idea that there is only one, conclusive public interest in any given context. Furthermore, it explicitly recognises, what many implicitly have understood as part of data protection legislation – that the protection of informational privacy is a public interest in itself.

2.4 Summary: what the public interest is and is not

To derive a legitimate approach to the public interest that is workable within a *legal* (and therefore normative) context, one must avoid certain conceptual vulnerabilities. The public interest must account for many component parts, which sometimes may conflict, including the views of individuals (majorities, minorities, and everything in between) and interests which transcend those individuals and exist at the group and societal level. The way in which these interests are resolved through decision-making practices impacts the legitimacy of any reliance on the public interest.

If we are to move towards more justifiable reliance on the public interest concept in data protection, we must accept that the public interest represents:

1) more than mere empirical facts, such as where the majority interest lies;
2) more than any single interest which may purport to be unanimous;

3) more than the outcome of any procedure and
4) more than what any single 'authority' may claim is justifiable in the public interest.

In the section below I set forth key components and changes to data protection legislation that can provide decision-makers with a means to engage with the substantive and normative qualities of the concept. The key components and legislative amendments suggested avoid the conceptual vulnerabilities identified above and are consistent with the aims of data protection law which are both protective and facilitative in nature.

3. Key Components of the Public Interest Concept

Below I introduce four key components to assessing the public interest in the processing of personal data. These components represent a new substantive understanding of the public interest concept in data protection. These components go beyond any previous contribution on this topic by combining the extensive legal and theoretical analysis undertaken in this thesis to offer a fuller outline of the concept in data protection. The components I suggest provide an understanding of the public interest that avoids the vulnerabilities identified and discussed in depth in Chapter 4, and reviewed above. On a practical level, the key components suggested below are translatable into guidance – a public interest checklist – for data controllers to assess the public interest in their processing (Section 3.5 below).

3.1 Contextual analysis required

A crucial component to making legitimate public interest determinations is that such decisions are first and foremost framed by the relevant *context*. This component is derived from the previous analysis on common interest theories and particularly influenced by Barry's understanding of 'publics' whereby:

> the qualifications for being 'a member of the public' vary from one situation to another, and we cannot therefore speak of what 'the public interest' requires until we know the particular context in which the question is being raised.[806]

[806] Barry (n 801) 504.

Within the limited but notable body of work addressing the public interest concept in data protection, the importance of assessing the concept in context is recognised.[807] Indeed, in Chapter 3, deep analysis of the legislative history to the DPD revealed a broad and contextual approach was intended for interpretation of the public interest provisions in Member States. In freedom of information law, even where strong public interest arguments are advanced for disclosure, it is the facts (and context) of each case which will determine the appropriate balance between withholding information and disclosure.[808]

Furthermore, in rejecting any absolute or unitary conception of the public interest concept, this also necessarily requires contextual analysis which is intertwined with the notion of who the 'public' is, in the public interest. Thus, in terms of data processing, this requires identification of the relevant public, or more often, *publics*. In any given data processing context, the publics which processing relates to, and or affects, will vary:

> …membership of the public is not fixed. It changes with the issue: the actors in one affair are the spectators of another, and men are continually passing back and forth between the field where they are executives and the field where they are members of a public.[809]

Therefore, the first key component of the public interest is the identification of:

> **What public or publics does the data processing in question relate to, and/or who may be affected by this processing?**

The idea of the 'public' is understood here to encompass both *a* public as 'a concrete audience, a crowd witnessing itself in visible space, as with a theatrical public' and *the* public as 'a kind of social totality…thought to include everyone within the field in question.'[810] By adopting an understanding of the public that encompasses *multiple* groups and individuals, decision-makers are steered away from flawed notions of the public interest as somehow equivalent to what they believe is the majority interest or

---

[807] Laurie (n 28) 279–282; Townend (n 28) 98–100; Taylor (n 28) 34. Also called for in the context of Article 8 jurisprudence: *Handyside* (n 386) para 48.
[808] ICO, 'The Public Interest Test: Freedom of Information Act' (n 651) 6.
[809] Walter Lippmann, *The Phantom Public* (10th edn, Transaction Publishers 2011) 100.
[810] Warner (n 50) 49–50.

is beneficial to the 'most' individuals (thus avoiding the weaknesses of preponderance theories). The notion of relevant *publics* directs decision-makers to a more nuanced and contextually sensitive analysis of the public interest. This can avoid the perpetuation of unsound theories (i.e. unitary theories) that conceive of the public interest as an immutable and static concept disconnected from the rights, interests and expectations of actual publics which are multiple. It also helps to avoid any conception of the public interest that is oppositional to the protection of informational privacy.

The relevant public or publics can be identified by determining whether:

- **Data being processed relate to them directly or indirectly; and/or**
- **They are affected, indirectly or directly, by the processing in question.**

The first prong to this test refers to the legal definition of personal data and therefore encompasses data which fall within the current scope of data protection law. The second prong to this test goes further and may avoid problems associated with the treatment of anonymised data as outside the scope of data protection law. The current legal dichotomy between 'personal' and 'anonymised' data does not account for harmful uses of the latter. Even if technically anonymous (or at least meeting the uncertain legal standard for anonymisation), anonymised data *can* be manipulated to cause real-life damage to specific individuals and groups, not to mention harm to broader societal interests in informational privacy.[811] This necessarily leaves out a wide array of data processing scenarios from legal scrutiny. While it is beyond the remit of this thesis to address these more fundamental defects within data protection law, the approach suggested recognises these and attempts to compensate, at least partially, for them specifically in context with reliance on the public interest conditions.

Thus the effect of processing must be understood more broadly than what data protection law currently recognises as 'harmful' data processing, and the law must *attach* to these wider circumstances.[812] The idea of 'effect' advocated for here encompasses

[811] danah boyd, Karen Levy and Alice Marwick, 'The Networked Nature of Algorithmic Discrimination'; Rauhofer (n 48).
[812] In work undertaken with colleagues for the Nuffield Council on Bioethics and Wellcome Trust's Expert Advisory Group on Data Access, we recommended a broader conception of harm be adopted

not just emotional distress or financial damage but wider effects that are subjectively felt and perceived by data subjects individually, or by groups, even if not formally recognised in the law.[813] Through a broader understanding of 'effect' in the data protection context, 'the public' in the public interest is afforded an interpretation which is less likely to leave any individuals or groups 'behind', at least in a procedural sense. As discussed in reference to preponderance theories (and to a lesser extent unitary theories), the public interest concept in data protection must be deployed in a way that is able to identify those situations where the protection of individual privacy must be prioritised over a case of public interest processing. Framing the question of *who* the relevant publics are by reference to who the processing relates to *as well as* those who may be affected (directly or indirectly), allows:

1) decision-makers to more readily identify whose expectations should be accounted for when determining whether a form of processing is justifiable on the basis that it is in public interest, and
2) facilitate the identification of cases where data processing must not proceed, to avoid the danger of perpetually placing the individual or smaller groups who may be disproportionately impacted from processing at risk of being outnumbered by a majority that may benefit, or favours, or simply does not object to, the data processing in question.

3.2 Public engagement to understand the impact of processing

Once data controllers have determined who the relevant publics are for a data processing initiative, they should engage with them to understand 1) what their expectations are and 2) any potential effects of processing which may not have been anticipated. As discussed in relation to preponderance theories, although empirical facts cannot fully populate the normative understanding required by a concept such as the public interest, public dialogue is important to identify the relevant interests and context surrounding a public interest decision. With the 'facts' (or preferences) gleaned from public dialogues, those that stand to be affected by a particular data processing initiative have at least *more* reason to believe that any decisions taken based on the

to encapsulate the myriad of ways individuals and groups may be affected by data processing but are not necessarily recognised formally in data protection law. Laurie and others (n 48).
[813] Similarly: ibid 41–46; Rauhofer (n 48).

'public interest' are not arbitrary or made on a whim. Whereas decision-makers (data controllers) will certainly have a *more* reasoned basis for making their decision.

However, it is not enough for a data controller to undertake a large-scale engagement exercise and simply report that 'x' number of people support 'y' data initiative. This would also be to fall prey to preponderance theories which wrongly equate the public interest with the majority interest. The results of a single public engagement exercise, no matter the sample size, can only ever represent the views and/or expectations of that particular public (at that time). It is unable to represent 'the' public interest because there is no singular public or public interest. While a vital source of information for data controllers, the results of public engagement (whether one or several) is not in itself dispositive of the issue of what is or is not normatively justifiable in the public interest.

Nevertheless, as Taylor indicates, there is a scarcity of understanding on the views of publics as to novel uses of their data, such as the reuse of genetic data for research.[814] Meaningful public engagement is particularly needed to inform our understandings of what is and is not acceptable when it comes to the reuse of data, when the reuse is not obviously related to the reasons for collection. Understanding publics' expectations is crucial to making informed and legitimate decisions which rely on the public interest to justify the reuse of data. Publics must be informed and engaged with regularly, and *prior to* the use of data. Justifying processing based on the public interest does *not* mean that data controllers relinquish their responsibilities to communicate and inform data subjects as to the processing of their data.[815] If anything, their duties to engage with their publics becomes heightened. And moreover, justifying processing based on the public interest conditions merely satisfies a data controller's obligations under the first data protection principle, that processing be lawful. It does not exempt data controllers from fair processing and other requirements under data protection law.

---

[814] Taylor (n 28) 34.

[815] The first data protection principle under the DPA 1998 requires that processing be both lawful *and fair*. Satisfying a condition under Schedule 2 (and Schedule 3 if processing sensitive personal data) only fulfils the requirement that processing be lawful; to be fair, among other things, would require that the data controller plainly communicate with data subjects about the processing of their personal data, especially when the purposes of processing differ from the original reasons for collection.

The frequently cited care.data debacle in England reveals that without meaningful public engagement, data initiatives can fail.[816] NHS England failed to adequately inform the public as to:

> …who will be able to access care.data for which purposes with which risks, how the credentials of bona fide researchers can be established, and what mandate commercial organisations will have to use data that originated from private consultations between patients and their GPs.[817]

NHS England similarly failed to articulate the benefits of the proposed scheme in a way that was meaningful and understandable to their publics.[818] The failure of care.data demonstrates the importance of communicating with the public *prior to* the undertaking of a new data initiative and the value in understanding the expectations of the relevant publics. Clearly communicating the intended benefits of a new data initiative is crucial where the public interest is the justification for processing. However, communication is only one aspect of public engagement.

Meaningful public engagement is a dynamic and two-way process: if public engagement reveals that a new use of data runs counter to the reasonable expectations of certain members of the public, that data controller must demonstrate how these views will be addressed within a robust framework of governance. Again, in considering the case of care.data, NHS England had not effectively communicated how individuals could opt-out of the scheme; their efforts at 'engagement' were strongly criticised and clearly did not have the intended effect as the scheme was eventually abandoned.[819] To engender a social licence to process personal data beyond the initial reasons for collection data controllers must demonstrate that their engagement efforts are not tokenistic. Thus, the second key component of the public interest is:

> **What are the reasonable expectations of the relevant public/publics as to uses of their data and how will these expectations be translated into the governance of those data?**

---

816 Carter, Laurie and Dixon-Woods (n 152).
817 ibid 407.
818 ibid.
819 ibid.

Meaningful public engagement will assist data controllers to understand the questions of 'effect' raised in the first component of the public interest suggested above. It will avoid accusation of capriciousness and arbitrariness; it will also avoid any perception that a data controller is claiming to be the ultimate 'authority' on what is and is not a public interest use of data (thus avoiding the dangers associated with unitary theories). The nature of established interactions between data controllers and 'their' public(s) (i.e. whether the interaction is developed in the private sector, charitable or public services context), will influence the expectations of said public(s). For example, in the case of public sector organisations (which are most likely to rely upon public interest justifications for processing[820]) the publics' reasonable expectations will be largely shaped by that organisation's governing legislation and mandate. What services do they provide? What is the nature of their interaction with individuals: voluntary or required by law? The nature of these interactions informs an important benchmark for public interest determinations: what are the reasonable expectations of the individuals, groups and wider public as they arise out of these interactions?[821]

Conflicts arise when data controllers decide to act in ways that are *contrary to* these reasonable expectations. The expectations of relevant publics are reasonable because they specifically arise out of the established conduct and character of interactions with a data controller. To avoid accusations of arbitrary and capricious use of the public interest ground for processing, data controllers' actions should be in accordance with these expectations unless such actions are necessary and justifiable. The key lesson taken from analysing Held's own conception of the public interest was her focus on the concept's approbative value – that its attachment to a particular statement or

[820] While Sch 2, para 5(d) technically provides that '*any* person' may justify the processing of personal data based on the public interest, that person must process data in regards to a function of a 'public nature'. The precise application of this provision remains untested in the UK courts, and therefore it remains uncertain how this might apply to third sector bodies or quangos. Under the equivalent provision in the forthcoming GDPR, Article 6(1)(e), it was again left to Member States to determine what type of data controller (public or private) may rely upon the provision. Under the GDPR, public authorities are explicitly forbidden from relying upon the legitimate interests' condition (Article 6(1)(f)) and thus are steered towards other justifications for processing, including consent, or the public interest condition. See Chapter 3 Section 3.1.2.

[821] Discussed in: Laurie and Stevens, 'Developing a Public Interest Mandate for the Governance and Use of Administrative Data in the United Kingdom' (n 63) 388.

decision expresses a level of justification, that 'x' ought to occur or that 'x' is defensible. In the present context, decisions to process data based on the public interest should be *justified* in terms of the potential benefits to accrue from processing, where the processing of data is necessary to deliver these benefits, which should *outweigh* any 'effect' upon the rights and interests of the relevant publics. This standard of justification is currently missing from the public interest conditions and must be added to our understanding of the concept if it is to have any normative and defensible meaning in data protection law.

New data initiatives will inevitably challenge pre-existing expectations and the mere fact that they *do* challenge these expectations does not necessarily mean this challenge is wrong. Rather, where data processing initiatives do counter existing expectations, the justifications for acting in this way must be subject to public scrutiny and data controllers should transparently set forth their reasoning in a forum of engagement *prior to acting*. Bright line rules cannot (and should not) be developed as to when the positive effects of data processing may outweigh any negative effects if we are to avoid the dangers associated with unitary theories of the public interest. What is critical and called for in this second component is that the publics' expectations are identified, considered and transparently accounted for *before* any decisions are taken based on the public interest. Only then could such decisions be said to be justified in the public interest.

3.3 The importance of transparent and legitimate procedures

The way public interest determinations are taken impacts upon the legitimacy of the public interest claim being made. The lack of an agreed decision-making process for relying upon the public interest has called into question the legitimacy of *any* reliance on the public interest conditions. As discussed in Chapter 2, this has privileged and perpetuated the consent-or-anonymise paradigm. While I have rejected any theory or outcome of procedure that claims to locate the public interest in a static, absolute or purely empirical sense, as both Taylor and Flathman argue, to be defensible a decision based on the public interest must be supported by *reasons* why 'x' is in the public interest

instead of 'y'.[822] Currently, data controllers are not required to (publicly) give any reasons for relying on the public interest condition (even if it would be ethical and legally prudent to do so); nor does the public interest condition for processing ordinary personal data explicitly require them to consider the impact of their processing vis-à-vis individuals/groups/society. Thus, I propose that third key component of the public interest is:

> **To be justifiable, a data controller's reliance on the public interest to process personal data must be based on the objective consideration of the impact of processing and this must be transparently documented and articulated to the relevant publics.**

This component can support data controllers in providing appropriate 'reasons' why 'x' processing is in the public interest. This can be best supported by the development of an agreed procedure for making public interest determinations when relying on the public interest conditions, something I propose in more detail in Section 4 below. This component advocates the idea that processing data is only *justifiable* in the public interest to the extent that a data controller can *demonstrate* reasons why processing is defensible on this basis, reasons which speak to the impact of processing and that are communicated transparently to those who stand to be affected. In this sense, pointing only to empirical facts such as the majority interest in a matter (preponderance theories), stating claims of apparent unanimity behind a particular cause for data processing (common interest theories) or appealing to a supposed superior or wise interest (unitary theories), would not be a defensible use of the public interest condition.

This third component and the procedures I suggest in Section 5 would support fuller consideration of the relevant contextual factors of data processing in a more objective and consistent basis than is currently the case. A clear procedure for making public interest determinations has certainly enabled the successful operation of the public interest test in the freedom of information context. The procedure this component suggests could provide clarity to a particularly ambiguous area of data protection law

---

[822] Flathman (n 573) 527–531; Taylor (n 28) 31.

and potentially instil confidence in data controllers to consider public interest justifications where consent and other avenues to lawfully process personal data are not open. The obvious question is: what should this procedure entail and how does it differ from current practice?

I have already answered at least part of this question with the key components suggested here and I will address this in more detail in Sections 4 and 5 below. Briefly, and on the broadest level, any agreed procedure would need to be informed *both* by 1) changes to the legislative provisions and 2) by authoritative guidance which in the UK would be provided by the ICO. Changes to the public interest conditions would substantively inform what legal standards should be deployed when assessing a data controller's reliance on these conditions. Guidance from the ICO would direct data controllers to the critical considerations of the public interest and offer key principles to guide their application of the legal standards to their own processing circumstances.

3.4 The public interest is a multiple concept

The development of a more transparent procedure for determining the public interest in data protection does not take away the importance of context which is crucial to understanding the concept. Indeed, I have explicitly rejected a purely processual understanding of the public interest; it is *more than* the outcome of an agreed procedure and requires *more than* substantiating compliance with that procedure. However, in also rejecting the prospect of unanimous, non-conflicting and absolute conceptions of the public interest, we are left with a conception that is potentially only descriptive (and essentially devoid of normative content). Where does this normative content come from, aside from the contextual (and situational) analysis required by my proposed first component? This content can and should be derived from theories of the public interest *and* from what is known of the intentions and aims of data protection law. From these sources, general principles of the public interest can be derived that are appropriate for assessing the public interest in data processing. The plausibility of this is evidenced from the principles offered in comprehensive guidance on the public interest test in the freedom of information context, which are derived from the intentions and aims of the relevant legislation.

What principles can be derived in the data protection context? Data protection law helps focus our attention on two broad public interests: the protection of informational privacy and in *some* uses of data – but crucially *neither* are absolute and both must be analysed in context. Thus, in principle, the public interest in each data processing scenario would be at least inclusive of 1) the public interest in protecting informational privacy (whether that be of the individuals to which the processing relates and/or will/could affect and 2) the public interest aim of processing. Within each of these two broad categories, could also be the interests/rights of groups, society and the private rights/interests of any of these, if processing is or is *not* undertaken. The number of public interest examples identified in data protection legislation is even further indicative of the multiplicity of interests at stake when considering the processing of personal data (and the limitless subject matter data processing can encompass). In recognition of this multiplicity of interests at stake in data processing, the fourth and final component is:

The public interest is *multiple*.

By starting any analysis of the public interest conditions from the position that there are at least *two* broad public interests at stake in any given situation recognises the inherent multiplicity of the public interest concept. It further supports the recognition that protecting informational privacy is a public interest in itself. Embracing the context sensitive and multiple nature of the concept avoids any use of it that may stake a claim to the public interest in a static or absolute sense to the detriment of other, and in particular, minority interests.

3.5 A public interest 'checklist' for data controllers

The proposed components of the public interest concept are directly translatable into a tool to guide data controllers through the decision-making process, when assessing the public interest in their processing. The components were derived from the theoretical analysis in Section 2 above specifically to avoid the conceptual vulnerabilities of the public interest, and therefore provide a means for data controllers

to engage with the difficult substantive and normative questions surrounding application of the concept to data processing. Translating theory into the key components, as illustrated in this checklist, can provide guidance to data controllers in a similar fashion to the guidance that has enabled public authorities to routinely apply the public interest test in the freedom of information context.[823]

The table on the following page translates the key components into a 'checklist' that 1) directs data controllers to the questions that should be asked when determining whether their processing is justifiable based on the public interest conditions and 2) highlights relevant factors, and those that are not typically dispositive, on whether the processing is ultimately (and normatively) justifiable in the public interest.

A checklist like this could be incorporated into any guidance developed by the ICO.

[823] See Chapter 5 Section 2.3.2.A-2.3.2.B.

Table 5 Public interest checklist for data controllers

Key component	Key questions	Relevant factors	Non-dispositive factors
1. Relevant publics	• What individuals does the dataset relate to? • What individuals, groups or publics are affected by the processing?	• Who is intended to benefit from the processing? • Who may be negatively affected (indirectly/directly) from the processing?	• That only a small number of people would be negatively affected vs a potential benefit to a larger group.
2. Reasonable expectations	• What steps have been taken to engage with the relevant publics? • What evidence do you have that indicates the relevant publics support *or* are likely to reasonably accept the intended processing?	• What relationship do you currently have with the relevant publics? (voluntary/legally mandated?) • Is the processing consistent with previous interactions? (i.e. is this use of data reasonably expected?) • How have you informed the relevant publics about the processing?	• That an engagement exercise was undertaken.
3. Objectivity & transparency	• This would be populated by the legislative procedures and ICO guidance suggested in Sections 3 and 4 below.	• How has the data controller complied with the legislative procedure and guidance?	• That relevant procedures are in place; evidence must support that they have been followed.
4. Public interest(s)	• How does the public interest in processing *outweigh* any counter public and private interests?	• How is informational privacy being safeguarded (technically and procedurally)? • What are the specific risks posed by this processing, whether to private or public interests? • What are the specific and intended benefits of processing? • What is the impact if processing is *not* undertaken?	• That risks to informational privacy have been mitigated; • Appeals to broad public interest arguments e.g. that because it is medical research, processing is justified on the public interest.

To implement the new understanding of the public interest suggested, legislative and procedural changes are required. Below I propose critical amendments to the public interest conditions in the DPA 1998.

4. Legislative Changes to the Public Interest Conditions

As discussed in Chapters 3 and 4, we currently lack any criteria or consistent procedure for assessing the public interest in processing beyond the descriptive examples in the legislation or relevant legal procedures.[824] The public interest conditions were included to justify various 'important' types of processing outside of consent and were to be interpreted and elaborated upon within the context of each Member State.[825] This task has been largely neglected in the UK context. The comparative analysis from Chapter 5 emphasised the integral and action promoting role of the public interest conditions and thus the need for clarity. Below I set forth ways in which UK legislation should change in line with the arguments made in this thesis regarding the newly developed understanding of the public interest concept. Even if there is little political appetite for further legislative changes to data protection law, considering the forthcoming GDPR and other more pressing items on the political agenda, the suggestions I make are what I contend is required to objectively and consistently deploy the public interest conditions.

4.1 Legislative change #1: Privileging informational privacy

Currently data controllers will *not* have to justify their reliance on the public interest conditions, only if and until their processing is the subject of disciplinary action by the ICO or a legal claim, (or questionable processing is brought to light in a public forum which instigates the intervention of the ICO and/or courts). Furthermore, the public interest conditions do not explicitly require data controllers to consider the effect of their processing on individuals, groups or broader interests. Thus, it is possible that potentially harmful processing which benefits *some* public but harms others may go unchecked if and until a legal claim is brought, by which time the damage may well be

[824] See Chapter 4 Section 3.2.
[825] See Chapter 3 Section 2.7.

done. As the status quo, this is patently unacceptable from an individual rights perspective but equally from the perspective of data controllers as they have not been equipped with the appropriate guidance to apply the public interest conditions in a way that is consistent with the aims of data protection law.

To direct data controllers to the relevant considerations, the protection of informational privacy must be *privileged* explicitly in the legislative provision. Such considerations must be built into the law if we are to move away from the current flawed thinking that informational privacy is merely an individual and not a public interest. This is also necessary if we continue to reject unitary theories which do not allow for multiple and valid but conflicting public interests to co-exist, which in data protection must be provided for. We see the success of this legislative approach from our consideration of the freedom of information context where disclosure is unambiguously privileged in the public interest test. Explicit recognition and privileging of the public interest in informational privacy would steer data controllers to consider the effect of their processing not only in terms of the impact upon specific individuals (potentially very few individuals) but also upon society, which has an interest in informational privacy being protected. Thus, the public interest condition for processing ordinary personal data could be revised to reflect the public interest of informational privacy:

> **The public interest in processing must outweigh any negative effect, direct or indirect, upon the public and private interests in protecting informational privacy, and any other public interests to not processing.**

This could also be introduced to qualify the Schedule 3 conditions for processing sensitive personal data based on the 'substantial' public interest, including those introduced by the DPPSPD 2000 such as for research. It is worth noting that my suggested legislative amendment is not beyond the bounds of reason. For example, in Germany, under the Federal Data Protection Act (*Bundesdatenschutzgesetz*) the processing of data for research is allowed if 'necessary' and 'where the scientific interest in carrying out the research project *substantially outweighs* the data subject's interest in excluding collection and the purpose of the research cannot be achieved in any other

way or would otherwise necessitate disproportionate effort.'[826] Further consider Australian privacy legislation (examined in Section 5 below) where the Information Commissioner can exempt certain uses of personal data on the basis that the public interest in processing data 'substantially outweighs' the public interest in abiding by the Australian Privacy Principles or a particular code of practice.[827]

My suggested reformulation places the burden of proof on data controllers to substantiate reasons why that the public interest in processing *outweighs* any counter effects on the public and private interests in protecting informational privacy (or considering any other public interest in *not* processing). Recall that in the freedom of information context, public authorities must substantiate reasons why the public interest in maintaining a qualified exemption *outweighs* the public interest in disclosure *because* disclosure is privileged within that legal context.[828]

Shifting the burden of proof to data controllers is justified in the context of data protection law, and specifically in the public interest conditions for similar reasons as proposed by Frederick Schauer in the human rights context: while rights such as privacy are often non-absolute, they 'are worth more than non-rights protected interests' such as the public interest in certain uses of data.[829] This suggests a reverse framing of our consideration of the public interest conditions:

Is the effect on informational privacy (and other public/private interests) justified in light of the public interest benefits the processing of data is expected to bring?

However, unlike the context of human rights law, which is *solely* focused on *protecting* individuals from interferences by the State, data protection law has dual aims which are facilitative in nature. Thus, it is crucial to remember that the reformulation suggested

---

[826] The Federal Data Protection Act (*Bundesdatenschutzgesetz*), s 13(2)(8). English translation available here: <https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html>(emphasis added).
[827] Federal Privacy Act 1988 (Australia), s 72(2).
[828] See Chapter 5 Section 2.1.
[829] Frederick Schauer, 'Proportionality and the Question of Weight', *Proportionality and the Rule of Law: Rights, Justification, Reasoning* (CUP 2014) 177.

here still presupposes '…that we assign weights to the gains and losses on *each* side of the equation'[830] – the effect of processing and the effect of *not* processing data.

By amending the legislation in this way, crucially, the presumption remains *in favour of* protecting informational privacy. It is *not* the case that the loss associated with the public interest pursued by 'x' processing may be no more than necessary than in light of protecting informational privacy.[831] Risk mitigation would not be enough, as is arguably the case under the legitimate interests condition.[832] Data controllers would need to demonstrate that they have not only accounted for potential effects (both direct and indirect) of their processing but that the public interest aims sought *outweigh* these potential effects, settling the inherently normative determination of deciding when processing is justifiable in the public interest. It offers the crucial and normative reasons why reliance on the public interest would be justifiable, if we recall Held's interpretation of the concept. The level of justification called for would require the data controller to engage in a more rigorous analysis of their proposed data initiative *before* relying upon the public interest conditions.

4.2 Legislative change #2: Introducing a standard of reasonable belief for public interest determinations

Even with the first legislative change suggested above, a key question remains unanswered: *how will a data controller's reliance on the public interest condition be assessed?* As argued throughout this thesis, public interest determinations are inherently context sensitive. However, data controllers must still initially decide the legal basis for processing based on their assessment of the issues. Currently, there is no prescribed

---

[830] ibid 180 (emphasis added).

[831] Argued by Schauer as to freedom of expression: 'The courts do not typically say that the loss in public order can be no more than necessary in light of the goal of pursuing freedom of expression, but they do say that the restriction on freedom of expression can be no more than necessary in light of the goal of pursuing public order.' ibid.

[832] Under the legitimate interests condition, data controllers may process personal data on the basis that it is necessary for their or a third parties' legitimate interests 'except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.' This is a substantially higher threshold of 'effect' ('unwarranted') than what I suggest for the reformulation of the public interest conditions - that the public interest benefit of processing *outweigh* any negative 'effect'.

standard for assessing a data controller's reliance on the public interest conditions nor on any other condition for processing.

We cannot derive a bright line rule defining when processing is justifiable based on the public interest if we are to avoid the conceptual vulnerabilities associated with (in particular) unitary theories. However, from our examination of whistleblowing legislation, we have learned that legal standards can play an important role in lending legal certainty to public interest determinations. The public interest test under whistleblowing law requires courts to consider whether the whistleblower *reasonably believed* their disclosure was in the public interest under a mixed test of reasonable belief.[833] A whistleblower is still protected by the law even if the public interest disclosure is wrong and/or there was no public interest in the disclosure being made, so long as the worker's belief (assessed subjectively), that it was in the public interest, was objectively reasonable.[834] Is it appropriate to also apply this mixed standard of reasonable belief to the public interest conditions in data protection law? If so, how would such a standard operate and would it improve the uncertainty surrounding the deployment of the public interest conditions?

4.2.1 Is a mixed test of reasonable belief appropriate?

To answer the first question, it is important to remind ourselves of the distinctions drawn between the public interest conditions in data protection and whistleblowing law where the reasonable belief standard is currently applied.

As opposed to whistleblowing law, the focus in data protection's public interest conditions is on the substantive and normative *content* of the 'public interest' claim. Is this processing *in* the public interest?[835] The applicability of the public interest condition for processing ordinary personal data rests upon the processing being 'necessary', related to a function of a 'public nature' and being substantively 'in' the 'public interest'. Therefore it would seem that if a court found that processing was *not* substantively 'in' the public interest, then another lawful basis would be required.

---

[833] ERA, s 43(b) as amended by the ERRA, s 17; *Chesterton* (n 774) [28]. See also note 784 above.
[834] *Chesterton* (n 774) [34].
[835] ibid [28].

Nevertheless, courts will always consider whether processing is in the public interest *based on the facts presented* and thus whether a data controller's reliance on the public interest condition was justified *in the circumstances*. Even if data protection law requires engagement with the *substance* of the public interest claim being made, on review, it is the *data controller's* consideration and/or demonstration of the public interest in processing that is assessed. It is the data controller that must make this initial assessment to determine the legal basis for processing. Thus, it is arguable that introducing a standard for making such assessments *is* appropriate and can lead to more consistent review of the public interest conditions.

4.2.2 How would a mixed test of reasonable belief operate?

To answer the second question, again, the operation of the reasonable belief standard in whistleblowing is instructive, where 'the word belief is subjective but the reasonableness of it is to be determined objectively.'[836] In data protection, it is the *data controllers*' assessment of their processing (and that it is justifiable 'in the public interest') that is subjective and akin to a worker's belief that a whistleblowing claim is in the public interest. Crucially, this *subjective* assessment of processing would need to be reasonable and this introduces an element of objectivity, just as in context with whistleblowing.[837] Thus, a further qualification must be added to the public interest conditions:

> **The data controller(s) must demonstrate their reasonable belief that the processing is in the public interest.**[838]

As to an argument that this legislative amendment 'lowers the bar' for relying upon the public interest conditions, I would counter that the wrong question is being asked. It is not a matter of lowering or raising standards, but ensuring that the right questions are being asked – that reliance on the public interest conditions are being scrutinised appropriately and in line with the protective *and* facilitative aims of data protection law.

---

[836] Lewis (n 784) 499. Citing *Babula* (n 773) [82], which provides for this 'mixed test' of reasonable belief (see note 784).
[837] *Babula* (n 773).
[838] This legislative amendment could equally apply to the Schedule 3 conditions for processing sensitive personal data and those introduced by the DPPSPD 2000.

It is data controllers' assessment of their processing circumstances that will be under review, either by the ICO or by a court. Thus I would argue that while the public interest in processing would still be assessed objectively in line with the current legislative provisions (that the processing is necessary, of a public nature and 'in' the public interest), it is appropriate and indeed sufficient that a data controller satisfy this mixed test of reasonable belief when relying upon the public interest conditions. To afford legal certainty to this assessment where there currently is none, this requires a standard that is explicitly provided within the law. Consider section 32 of the DPA 1998 where the reasonable belief standard is already deployed in relation to the public interest:

> (1) Personal data which are processed only for the special purposes are exempt from any provision to which this subsection relates if—
> (a) the processing is undertaken with a view to the publication by any person of any journalistic, literary or artistic material,
> (b)*the data controller reasonably believes that, having regard in particular to the special importance of the public interest in freedom of expression, publication would be in the public interest*, and
> (c)the data controller reasonably believes that, in all the circumstances, compliance with that provision is incompatible with the special purposes.[839]

The ICO has dedicated guidance to interpreting the public interest and reasonable belief requirement in section 32, which advises data controllers in the media to have clear and documented reasons why publication is in the public interest (this is reflected both in the ICO's evidence to the Leveson inquiry on the use of section 32, as well as in the subsequent 'guide for the media'.[840] It is worth noting, that the reasonable belief standard in section 32 is not without its controversy. After the Leveson inquiry, the Information Commissioner indicated that the standard could restrict the ICO's enforcements powers vis-à-vis the media, given that the ICO would have limited power to investigate or challenge a journalist's reasonable belief. It is arguable that introducing a mixed test of reasonable belief might have a chilling effect on enforcement where the

---

[839] DPA 1998, s 32(1).
[840] The Right Honourable Lord Justice Leveson, 'The Leveson Inquiry: An Inquiry Into the Culture, Practices and Ethics of the Press' (2012) Volume 3 1063 <http://webarchive.nationalarchives.gov.uk/20140122145022/http://www.official-documents.gov.uk/document/hc1213/hc07/0780/0780_iii.asp>; ICO, 'Data Protection and Journalism: A Guide for the Media' (n 251) 32.

public interest condition is relied upon. However, the legal certainty offered by introducing such a standard, along with the guidance and procedures recommended in this thesis, are what I consider is needed to overcome the current gaps in understanding which are detrimental to both public interest uses of data *and* to the relevant publics. Furthermore, the guidance and procedures recommended in this thesis would require data controllers to document their reasons for believing their processing is in the public interest (similar to best practice in freedom of information). Having such documentation readily available would allow the ICO to focus on the heart of the issue i.e. whether reliance on the public interest condition to processing was reasonable or not.

Similarly, as discussed in the freedom of information context, the ICO advises that public authorities document their arguments for and against disclosing information under the public interest test, resembling an objective standard of assessment.[841] By introducing a *mixed* test of reasonable belief as a qualification to the public interest conditions, explained in ICO guidance, data controllers would be directed to a more objective consideration of the range of public interests at stake in any given processing context whilst allowing for the relevant contextual factors to also be taken into account. As a final point, it is worth noting that mixed tests of reasonable belief are not unusual in law.[842] The observations made here (and originally in Chapter 5) contribute to an understanding of how data protection law might be amended to address the gaps in practice and procedure identified through my analysis of the public interest.

---

[841] ICO, 'The Public Interest Test: Freedom of Information Act' (n 651) 9.

[842] For example, mixed tests of reasonable belief are used in various criminal defences. For certain sexual offences, the accused's belief that the complainant consented must be objectively reasonable but is balanced against subjective considerations as to whether the complainant had capacity to consent in the circumstances. As a further example, in cases where self-defence is claimed, the jury will consider 1) whether the accused *subjectively* believed the use of force was necessary and reasonable and 2) whether based on the facts of the case as the accused believed them to be, whether a reasonable person would consider the force used as reasonable or excessive.

4.2.3 Would introducing a mixed test of reasonable belief improve legal certainty?

Introducing a mixed test of reasonable belief *would* provide data controllers with more legal certainty. They could better anticipate how their reliance on the public interest conditions would be assessed, by both the ICO and courts, and could make their decisions to process personal data accordingly. It would be in data controllers' best interests to document their consideration of the effect of processing on informational privacy along with any impact from *not* processing. For example, data controllers could document their answers to the questions posed in my public interest checklist. Their reliance on the public interest conditions would be assessed based on their reasons why the public interest in processing outweighs any counter interests (public or private). Data controllers could be assured that if their answers are objectively reasonable (while their belief would be subjectively assessed), that their reliance on the public interest conditions would be considered legitimate. From a data subject's perspective, introducing this standard would support a more balanced consideration of whether reliance on the public interest is justified. The public interest checklist and accompanying documentation could explicitly demonstrate how a data controller has considered and addressed the effects of processing, on either side of the argument.

More broadly, by introducing the standard into the legislation itself, the action-promoting role of the public interest conditions would be better supported. As discussed throughout this thesis, the role of the public interest conditions are misinterpreted as 'exceptions' to obtaining consent, when my examination of the legislative history to the DPD and DPA 1998 demonstrates that this is not the case.[843] Furthermore, drawing from my consideration of the public interest defence in copyright, it is critical to clarify and support the function of the public interest conditions as action promoting which requires a level of detail that is more appropriately addressed in legislation and authoritative guidance rather than being an ad hoc task for the courts.[844]

---

[843] See Chapter 3 Section 2.7.
[844] See Chapter 5 Sections 3.1.4 and 3.2.

As the public interest conditions are *not* fail-safe exemptions from obtaining consent, nor from a data controller's other obligations under the DPA 1998, it is certainly appropriate to provide *more* detail and instruction as to how reliance on the condition would be assessed, not least because data controllers must determine their legal basis for processing. This contrasts with the public interest defence in copyright which remains relatively undefined due to the more limited role prescribed to it within the CDPA, as confirmed by the courts. Introducing a clear standard of assessment for reliance on the public interest conditions would explicitly indicate to data controllers the conditions as 'reasonable' (and not merely failsafe exceptions) to rely upon if the relevant qualifications are satisfied.

In summary, introducing a mixed test of reasonable belief for assessing reliance on the public interest conditions would help to initiate important but incremental changes to how data controllers conceive of their justifications for processing personal data, including when appropriate, based on the public interest. Introducing this standard and implementing it through routine use of an agreed decision-making procedure (an example being the public interest checklist) would incentivise data controllers to routinely identify and document their consideration of the public and private interests implicated by their processing when relying on this legal basis. Thus, data controllers would be directed to a more consistent and transparent basis for taking public interest decisions, which is crucial if such decisions are to be legitimate. Such an approach is clearly possible, given the successful deployment of the reasonable belief standard in the whistleblowing context. A summary of my revised public interest condition for processing ordinary personal data is as follows (added onto the current provision in Schedule 2 paragraph 5(d):

The processing is necessary:
(d) for the exercise of any other functions of a public nature exercised in the public interest by any person.

The public interest in processing must outweigh any negative effect, direct or indirect, upon the public and private interests in protecting informational privacy, and any other public interests in not processing.

The data controller(s) must demonstrate their reasonable belief that the processing is in the public interest, where the reasoning will be assessed objectively and belief assessed subjectively.

In Section 5, I suggest two alternative procedures to deploy the new understanding of the public interest and accompanying legislative amendments.

5. New Procedures for Making Public Interest Determinations in Data Protection Law

How would data controllers, the ICO and courts implement the key components of the public interest and recommended legislative amendments? I suggest two alternative procedures which could improve how public interest determinations are initially made by data controllers and later direct how the ICO and courts would scrutinise data controllers' reliance on the public interest conditions. These procedures are:

1. **A code of practice for public interest determinations**: if data controllers document their compliance with the code of practice on the public interest conditions, upon regulatory intervention by the ICO or judicial review, this could be used as evidence of compliance with data protection law.

2. **Administrative authorization outside the judicial process**: the ICO could provide data controllers with a 'stamp of approval' (authorization) to process personal data on the basis that it is in the public interest for certain processing circumstances. This authorization could provide a presumption of compliance with data protection law upon judicial review.

When presenting each procedure, I will consider it in terms of: 1) the data controller's initial decision to process personal data; 2) any ICO intervention; and 3) judicial review.

5.1 A code of practice for public interest determinations

My first proposed procedure is premised on the idea that data controllers begin to routinely apply and document their use of a decision-making procedure set forth in authoritative ICO guidance applicable to the public interest conditions – a 'code of practice' for making public interest determinations. A data controller could document their consideration of the issues presented by the code of practice, which could be considered by the ICO or courts as evidence of legal compliance, upon future complaints or commencement of adjudicative processes.

5.1.1 Guiding the data controller's initial decision to process personal data

To implement this new procedure, first, relevant guidance would need to be produced by the ICO which explains to data controllers how to assess the public interest in their processing. The key components of the public interest concept and the public interest checklist are examples of what could form the basis of a 'code of practice' on the public interest conditions. The key components of the public interest (suggested in Section 2) provide guiding principles which are accompanied in the checklist by more context-specific questions, which data controllers could use to assess their processing. Thus, the checklist exemplifies a potential decision-making procedure. Within the code of practice, the ICO could add further examples where the public interest conditions have been successfully (or unsuccessfully) relied upon, based on the ICO's extensive and ongoing engagement efforts with data controllers (more on this in Section 6 below). As considered in Chapter 5, with regards to freedom of information law, the provision of guiding principles and context specific examples in authoritative guidance, is crucial to enabling decision-makers to independently assess the public interest.

Second, a further legislative change would be required to direct data controllers to this guidance, but also to create the statutory impetus for the ICO to produce it and to enable both the ICO and courts to consider abiding by the code of practice as evidence of compliance. There is already precedent for such a procedure in context with the exemptions for journalism, literature and art under section 32 of the DPA 1998:

> …whether the belief of a data controller that publication would be in the public interest was or is a reasonable one, regard may be had to his compliance with any code of practice which—
> (a)is relevant to the publication in question, and
> (b)is designated by the [F1 Secretary of State] by order for the purposes of this subsection.[845]

Here, the relevant codes of practice are developed by industry and include the Editors' Code of Practice, the Ofcom Broadcasting Code and the BBC's Editorial Guidelines.[846] Data controllers are incentivised to comply with the codes of practice as this may be considered (favourably) as evidence of legal compliance. A similar addition could be added as a further qualification to the public interest conditions. Thus, my revised public interest condition to processing ordinary personal data would now read:

The processing is necessary:
(d) for the exercise of any other functions of a public nature exercised in the public interest by any person.

The public interest in processing must outweigh any negative effect, direct or indirect, upon the public and private interests in protecting informational privacy, and any other public interests to not processing.

The data controller(s) must demonstrate their reasonable belief that the processing is in the public interest, where the reasoning will be assessed objectively and belief assessed subjectively.

Whether the reasoning of a data controller that processing is in the public interest was or is objectively reasonable, regard may be had to his compliance with any code of practice which—
(a)is relevant to the processing in question, and
(b)is designated by the [Secretary of State] by order for the purposes of this

Considering the lessons learned from examining the public interest defence in copyright, and thus the risk of leaving interpretation of the public interest conditions to the courts, providing this level of detail within the legislation is necessary. This is because: 1) the role of the public interest conditions are *action promoting* as opposed to

---

[845] DPA 1998, s 32(3).
[846] 'Editors' Code of Practice' (*Independent Press Standards Organisation*, 2016) <https://www.ipso.co.uk/editors-code-of-practice/>; 'The Ofcom Broadcasting Code (incorporating the Cross-Promotion Code)' (*Ofcom*, 2016) <https://www.ofcom.org.uk/tv-radio-and-on-demand/broadcast-codes/broadcast-code>; 'Editorial Guidelines' (*BBC*, 2016) <http://www.bbc.co.uk/editorialguidelines/guidelines>.

being a fail-safe exemption or defence and 2) data controllers must independently make these determinations in the first instance. To 'benefit' from the code of practice, data controllers would need to substantiate their use of it. Here, the ICO's guidance on the application of section 32 is informative. There, the ICO suggests the following documentation:

> In practice, we are likely to accept there was a reasonable belief that publication was in the public interest if an organisation:
> - has clear policies and procedures on public interest decisions,
> - can show that those policies were followed,
> - can provide a cogent argument about the public interest, and
> - has complied with any relevant industry codes.[847]

The ICO goes on to list factors which may indicate a data controller's assessment of the public interest was *not* reasonable:

> Organisations might find it more difficult to rely on the exemption if:
> - they have no clear policies or procedures,
> - journalists acted outside of company policies or accepted practice,
> - there is no evidence that anyone thought about the public interest, or
> - an industry body finds them in breach of a code of practice.[848]

Such guidance can be adapted to the public interest conditions. This would explain to data controllers the purpose of the code of practice and broadly what is expected of them when relying upon the public interest conditions:

> **In practice, we are likely to accept there was a reasonable belief that the processing was in the public interest if the data controller:**
> - **has clear policies and procedures on public interest decisions,**
> - **can show that those policies were followed,**
> - **can provide a cogent argument about the public interest, and**
> - **has complied with this code of practice, including the public interest checklist.**
>
> **Data controllers might find it more difficult to rely on the public interest conditions if:**
> - **they have no clear policies or procedures,**

[847] ICO, 'Data Protection and Journalism: A Guide for the Media' (n 251) 36.
[848] ibid.

- **the processing of data is undertaken contrary to the relevant policies,**
- **there is no evidence that anyone thought about the public interest, or**
- **the ICO determines the processing is in breach of this (or any other relevant) code of practice.**

In considering the key components to the public interest presented in Section 2, and the importance of transparent procedures subject to public scrutiny, any documentation could be made available on the data controller's website and potentially on the ICO's website. As to the latter option, this could create a central 'register' of data processing activities that are justified on the public interest conditions. However, this may be more relevant for processing which has been specifically reviewed and 'authorised' by the ICO, a procedure considered in Section 5.2.[849]

5.1.2 Evidence of legal compliance upon ICO intervention

Abiding by the code of practice could be used by data controllers as evidence of legal compliance with the first data protection principle if complaints were later investigated by the ICO. As the author of the code of practice, the ICO would be in the prime position to investigate the extent to which the data controller appropriately applied the guidance and may already have a history of interactions with the data controller to guide an assessment of the circumstances. In the freedom of information context, the ICO routinely assesses public authorities' application of the public interest test and has generated a consistent approach to making decisions on this area of the law.[850] The ICO's adoption of a decision-making procedure, akin to my suggested public interest checklist, could play a role in generating a consistent approach to the review of what is a currently unsettled and particularly ambiguous area of data protection law.

5.1.3 Evidence of legal compliance upon judicial review

A data controller's compliance with the code of practice could also be used as evidence of legal compliance upon judicial review. As discussed above, there is already precedent for this is in data protection law in the exemptions for journalism, literature and art,

---

[849] Indeed, this is the case with public interest determinations for processing personal data, authorised under Australian privacy legislation. See Section 4.2 below. Australian Government Office of the Australian Information Commissioner, 'Public Interest Determinations: Privacy Registers' (2015) <https://www.oaic.gov.au/privacy-law/privacy-registers/public-interest-determinations/>.
[850] See Chapter 5 Section 2.3.

where the relevant codes of practice are developed by industry.[851] This contrasts with the code of practice suggested here, which would be developed by the ICO.

The ECtHR in *Mosley v United Kingdom* paid significant attention to the section 32 exemption and were thusly directed to the codes of practice applicable to the UK media; these influenced their determination that there was *not* a violation of Article 8 of the ECHR in the absence of the UK imposing a duty on the *News of the World* to pre-notify Mosley prior to publication.[852] As the adjudicative process would normally commence *after* any intervention of the ICO (in a data protection claim), the courts *could* make use of the ICO's findings on a data controller's compliance with the code of practice before making a final judgment. However, the recommendation being made here would certainly not preclude the judiciary from coming to an alternative conclusion than the ICO (or indeed the data control). If the code of practice integrates the mixed test of reasonable belief suggested above, it is possible that a UK court would defer to the approach taken in *Mosley* to the reasonable belief standard vis-à-vis a public interest claim:

> The Court considers that in order to prevent a serious chilling effect on freedom of expression, a reasonable belief that there was a 'public interest' at stake would have to be sufficient to justify non-notification, even if it were subsequently held that no such 'public interest' arose.[853]

This approval of the reasonable belief standard would of course only apply to the extent that a data controller could also demonstrate that the public interest in processing *outweighed* the public and private interests in protecting informational privacy and any other public interests in not processing (in line with the legislative change suggested in Section 3.1 above).

Any argument that this type of code of practice takes significant elements of interpretation of an important legal concept outside parliamentary scrutiny, and potentially, judicial review is easily addressed by reiterating the circumstances

---

[851] 'Editors' Code of Practice' (n 846); 'The Ofcom Broadcasting Code (incorporating the Cross-Promotion Code)' (n 846); 'Editorial Guidelines' (n 846).
[852] *Mosley v United Kingdom* App no 48009/08 (ECtHR, 12 April 2012).
[853] *Mosley* (n 852) [126].

surrounding the current lack of guidance and interpretation on the public interest conditions. As discussed throughout this thesis, neither the DPD nor DPA 1998 define the public interest aside from the provision of examples (where political motivations featured strongly and objective criteria were lacking). Furthermore, it is the data controller that must initially decide their legal basis for processing, and thus, where relevant, whether their processing meets the requirements of the public interest condition. The provision of *any* guidance for public interest processing could only be beneficial considering the types of processing and potential societal impacts at stake. As suggested, compliance with the code of practice could serve as *evidence* of compliance with Schedule 2 and Schedule 3, but would not be dispositive nor supplant the judiciary's right to override a data controller's determination on the matter. Ultimately the public interests at stake are best served by the provision of guidance where there currently is none, regardless of the legal status of the code of practice.[854]

5.1.4 Benefits of a code of practice for public interest determinations

There are several benefits to introducing a code of practice for public interest determinations, and subsequently using a data controller's application of it as evidence of legal compliance. First, the introduction of the code of practice would enhance legal certainty for data controllers. It would highlight the relevant considerations for data controllers' initial (and unsupervised) decisions on determining a legal basis for processing (set forth in my public interest checklist), while alerting them to the processing circumstances which would be unlikely to meet the relevant legal conditions. It would also provide an element of foreseeability as a data controller's use of the code of practice could become a source of evidence of legal compliance upon regulatory intervention or judicial review.

---

[854] The issue of the proper distribution of power between Parliament, courts and other administrative bodies, lies beyond the scope of my thesis. However, the suggested code of practice remains within the bounds of the UK's unique political settlement. To address this in full would require a different debate entirely, to analyse if judicial review is still fit for purpose. If the ICO is legally obligated to draft the code, it is itself, as a public authority, subject to judicial review in terms of whether the code of practice complies with the DPA and general administrative law requirements. There are also non-data protection law examples of a court being forced to take compliance with (in this case a non-statutory) code into account – see Section 12(4) Human Rights Act 1998 and, for example *Max Mosely v News Group Newspapers Ltd* [2008] EWHC 1777 (QB), [16], [110], [141] and [144].

Second, by introducing the code of practice and referring to it explicitly in the legislation, the transparency of public interest determinations will be promoted beyond the currently uncertain means in which public interest decisions are taken. Moreover, if data controllers place their code of practice documentation online, this provides data subjects and relevant publics an opportunity to scrutinise these otherwise opaque decision-making processes.

Third, the introduction of the code of practice and its availability as evidence of legal compliance could help initiate incremental culture change surrounding the use of personal data in the UK. The current culture is risk averse and predisposed to several legal myths including that the public interest conditions are exemptions to consent. Once the principles espoused in the code of practice became routinely applied by data controllers and consistently assessed by the ICO and courts, legal uncertainty could be diminished, contributing to a more holistic perspective on the protective and facilitative aims of data protection law, beyond consent or anonymisation.

Fourth, and finally, introducing the code of practice is a 'resource light' option, and already within the remit and capabilities of the ICO. As discussed, the ICO has already produced comprehensive guidance on matters of the public interest in the freedom of information context and even in data protection on the section 32 exemptions. Using these as a template, the introduction of a code of practice and its role in substantiating evidence of legal compliance is a procedure which is potentially highly beneficial, vis-à-vis the relatively little resources required to deploy it.

5.2 Administrative authorization of public interest determinations

The second procedure suggested is the extrajudicial authorization of public interest determinations in advance of *certain* forms of particularly risky, novel, pervasive or unexpected processing (from the perspective of data subjects/publics). The ICO would assess applications to justify such processing based on the public interest conditions. The ICO could 'authorize' a data controller to process personal data based on satisfaction that the public interest conditions have been correctly applied to the processing circumstances.

An analogous procedure already operates successfully within England, with the reuse of health data for research, audit and other medical purposes. The Confidentiality Advisory Group ('CAG') is an independent body of experts (established by the UK's Health Research Authority ('HRA')[855]) that advises the relevant decision-makers[856] on whether it is ethical and appropriate to reuse patient data, without consent, for a purpose such as research. CAG assess applications based on '…whether the activity is in the public interest, if it fulfils a medical purpose, and that there is no other reasonable way in which to carry out the activity'.[857]

However, even more similar to what is being suggested here is the Australian procedure for making public interest determinations ('PIDs') under federal privacy legislation.[858] The Australian Information Commissioner can make a PID which provides that an act or practice that would otherwise breach an Australian Privacy Principle, or relevant code of practice, will not be regarded as having done so.[859] PIDs are made on the basis that:

> …the public interest in the entity doing the act, or engaging in the practice, substantially outweighs the public interest in adhering to that code or principle;

---

[855] The HRA was established in 2011 as part of the Care Act 2014 to '…protect and promote the interest of patients and the public in health and social care research, co-ordinate and standardise practices relating to regulation, recognise and establish Research Ethics Committees (RECs), be a member of UK Ethics Committee Authority (UKECA), promote transparency in research and provide approvals for the processing of confidential information relating to patients.' 'About Us' (*NHS: Health Research Authority*) <http://www.hra.nhs.uk/about-the-hra/>.

[856] In England and Wales, this would be the Secretary of State for Health or HRA, that can approve applications to use identifiable patient data without consent. Health Service (Control of Patient Information) Regulations 2002, SI 2002/1438.

[857] NHS HRA, 'Recommendations and Approval Decisions' <http://www.hra.nhs.uk/documents/2014/02/cag-frequently-asked-questions-3.pdf>.

[858] A similar procedure applies under Section 31 of Victoria's Privacy and Data Protection Act 2014 and in New South Wales under Section 41 of their Privacy and Personal Information Protection Act 1998. Commissioner for Privacy and Data Protection State Government of Victoria, 'Guidelines to Public Interest Determinations, Temporary Public Interest Determinations, Information Usage Arrangements and Certification' (2014) <https://www.cpdp.vic.gov.au/images/content/pdf/Guidelines_to_Public_Interest_Determinations.pdf>; Office of the Australian Information Commissioner (n 849); 'Public Interest Directions' (*Information and Privacy Commission New South Wales*, 2016) <http://www.ipc.nsw.gov.au/public-interest-directions>.

[859] Privacy Act 1988 (Australia), s 72(2).

> the Commissioner may, by legislative instrument, make a determination to that effect.[860]

The Australian experience can be used to inform the discussion below.

5.2.1 Data controller preparations for authorization

Under this authorization procedure, data controllers could apply to the ICO to approve their processing of personal data based on the public interest conditions. This contrasts with the current process whereby data controllers *independently* determine their legal basis for processing, possibly with the assistance of legal counsel and/or an in-house data protection officer. These initial data controller decisions are not assessed by the ICO or any other official body: they only are scrutinised if legal complaints are later lodged and/or the ICO is prompted to investigate a data controller's processing operations. Authorization would require further legislative changes and a set procedure for 1) determining how applications should be put forward, 2) how they will be assessed and 3) how the outcome of an application can be contested. For these purposes, the Australian procedure for making PIDs is instructive.

The Australian Information Commissioner can make a PID on the basis that the public interest in a use of data 'substantially outweighs' the public interest in complying with the legislation and/or a relevant code of practice.[861] The purpose of a PID is to exempt a use of data from a particular legislative provision or a relevant code of practice.[862] The Privacy Act 1988 details:

- who may apply for a PID;[863]
- the circumstances in which the Information Commissioner may make a PID;[864]
- the legal effect of providing a PID;[865]
- how applications are to be assessed;[866]

---

[860] ibid s 72(2)(b).
[861] Privacy Act 1988 (Australia), s 72(2).
[862] ibid s 72(2)(a)(i)-(ii).
[863] ibid ss 71, 73.
[864] ibid ss 72, 73.
[865] ibid s 72(3)-(5).
[866] ibid ss 72(2), 73(1)(A), 78, 79.

- that applications should be published with the consent of the applicant;[867]
- a process for the applicant and the Commissioner to consider a 'draft' PID before the final determination is made;[868]
- a process for inviting the public to consider and make comments on the application to the Commissioner;[869]
- a process for making 'temporary' PIDs which are only effective for a period of up to 12 months;[870] and
- that a register of PIDs must be maintained and made available to the public.[871]

Considering the legal ambiguity surrounding the current iteration of the public interest conditions, the lack of ICO guidance and interpretative case law, I suggest a similarly robust procedure to the Australian system be *explicitly* provided for in amended UK data protection legislation.

The data processing circumstances in which this procedure may be particularly useful is when a form of processing is determined by the data controller to be particularly 'risky', in terms of the potential negative affect/impact on individuals, groups and/or society. This level of risk could be determined by the data controller during their routine privacy impact assessments for new processing operations, in light of the potential for the processing to cause physical, emotional, financial or reputational harm or even harms to wider public interests (e.g. damaging confidence in a particular public service).[872] If we think of the case of care.data, or more recently, the research initiative involving Google DeepMind and London's Royal Free Hospital,[873] one could also

---

867 ibid s 74.
868 ibid s 75.
869 ibid ss 76, 77.
870 Privacy Act 1988 (Australia), ss 80(A)-(B), (D).
871 ibid s 80(E).
872 In other work, myself and colleagues conducted an evidence review triangulating the cause and effect (harms) of types of personal data misuse. Our review revealed a broad range of potential harms that can befall an individual if their personal data are misused. For the present discussion, it is important to consider 'risk' and 'harm' as it relates to data processing in a much broader sense than currently understood in data protection legislation (where harm is typically connected to being able to prove actual harm or financial damages). When determining whether authorization is appropriate, this broader understanding of harm should be referred to. Laurie and others (n 48) 50.
873 Where Google's DeepMind were provided London Royal Free Hospital patient records to develop an app that would alert doctors to patients at risk for acute kidney injuries. In May 2017, a letter from the UK's National Data Guardian (Dame Fiona Caldicott) to the Royal Free NHS Trust and to DeepMind, was leaked; this letter indicated that implied consent was claimed by the parties as the legal

imagine that authorization may be appropriate where particularly novel and pervasive data processing initiatives are proposed, which may be unexpected from the perspective of data subjects and publics in terms of factors such as the scale, and who will be conducting the processing (such as a private company as opposed to the public sector body in question). In this sense, and following on from the brief discussion of purpose limitation in Chapter 2, one could imagine that such an authorization procedure might also be used to determine compliance with *other* data protection requirements such as the compatibility of reuses of data.[874]

Nevertheless, to avoid disproportionate impact on the processing of data for research, a concern raised throughout this thesis, it would be important that ICO authorization should not be a mandatory requirement. Instead, it could operate as another (invaluable) tool for data controllers to use, as part of their entire pre-processing risk and compliance assessment. Where a data controller wishes the additional comfort of ICO authorization in advance, it should be possible to apply for this. It could be expected that such authorization would be sought only where there are risk thresholds met or other serious concerns raised which warrant this level of regulatory intervention. Particularly when considering the processing of personal data for research, not only are individuals' data protection rights and freedoms at stake, but also individuals' rights and freedoms as to the arts and sciences guaranteed by Article 13 of the CFR[875]. Therefore, pragmatism and risk-based assessment are crucial to applying the proposed authorization procedure. Given the broad understanding of personal data, [876] it is

basis for sharing but that this was invalid. Jane Wakefield, 'Google DeepMind's NHS Deal under Scrutiny' (*BBC News*, 17 March 2017) <http://www.bbc.co.uk/news/technology-39301901>; Natasha Lomas, 'DeepMind NHS Health Data Deal Had "no Lawful Basis"' (*TechCrunch*, 15 May 2017) <https://techcrunch.com/2017/05/15/deepmind-nhs-health-data-deal-had-no-lawful-basis/>.

[874] As indicated in Chapters 1 and 2 it is critical for the reader to understand that the focus of this thesis is on the application of the public interest conditions to processing; whether a form of processing falls awry of *other* data protection provisions is not the subject of this thesis.

[875] Given my focus on research processing based on the public interest conditions, this clearly implicates Article 13 of the CFR where 'The arts and scientific research shall be free of constraint. Academic freedom shall be respected.'

[876] In its guidance for journalism, the ICO provides that '…information does not have to be 'private' to be personal data. Anything about a person can be personal data, even if it is innocuous or widely known. For example, a public figure's job title can be personal data, as can a photograph taken in a public place, a listed phone number, or information posted online.' As such, a pragmatic and risk based approach would be appropriate to determine when authorization may be required. ICO, 'Data Protection and Journalism: A Guide for the Media' (n 251) 22.

neither desirable nor necessary for *every* reliance on the public interest condition to require prior authorization. For particularly novel and large scale research initiatives, however, the legal certainty it would provide would be a useful improvement upon the current ambiguity when it comes to the application of the public interest conditions to research.

The authorization procedure could be added as an additional Schedule to the DPA 1998 and my suggested draft of this is provided on the following pages based on the Australian legislation[877].

Part I – Public Interest Authorizations

1. Interpretation

(1) For the purposes of this Schedule, a data controller is interested in an application being made under paragraph 3 if, and only if, the Information Commissioner is of the opinion that the data controller has a real and substantial interest in the application.

2. Power to make, and effect of, authorizations

Authorization of processing based on Schedule 2, paragraph 5(d)

(1) The Information Commissioner may authorise processing based on Schedule 2, paragraph 5(d) if he or she is satisfied that:
(a) the processing of personal data satisfies the conditions of paragraph 5(d), and
(b) the public interest in the processing of personal data outweighs the public and private interests in protecting informational privacy and any other public interest against processing.

Effect of an authorization under subsection (1)

(2) The data controller is taken to have satisfied Schedule 2, paragraph 5(d) if processing occurs while the authorization is in force under subsection (1). Upon regulatory intervention by the Information Commissioner or in subsequent judicial proceedings, lawfulness, as required by Schedule 1, paragraph 1, may be presumed in light of the authorization made under this Schedule.

3. Application by a data controller

(1) A data controller may apply for an authorization of processing based on Schedule 2, paragraph 5(d) subject to paragraph 1.

(2) If:
(a) an application is made under subsection (1); and
(b) the Information Commissioner is satisfied that the application is frivolous, vexatious, misconceived, lacking in substance or not made in good faith, the Information Commissioner may, in writing, dismiss the application.

(2) The Information Commissioner shall create and disseminate guidance which explains:
(a) the procedure and format of the application process; and
(b) the basis upon which applications are assessed.

4. Publication of application etc.

(1) Subject to subsection (2), the Information Commissioner shall publish, in such manner as he or she thinks fit, notice of:
(a) the receipt by the Information Commissioner of an application; and
(b) if the Information Commissioner dismisses an application under paragraph 3(2)—the dismissal of the application.

(2) The Information Commissioner shall not, except with the consent of the data controller, permit the disclosure to another body or person any information contained in a document provided by the data controller as part of, or in support of, an application made under this Schedule if the data controller has

[877] Adapted from Part VI of the Privacy Act 1988 (Australia).

informed the Information Commissioner in writing that the data controller claims that the document is exempt from disclosure within the meaning of the *Freedom of Information Act 2000* or the *Freedom of Information (Scotland) Act 2002*, or subject to any other legal obligation to withhold the information or otherwise keep the information confidential .

5. Draft authorization

(1) The Information Commissioner shall prepare a draft of his or her proposed authorization in relation to the application unless he or she dismisses the application under paragraph 3(2).

(2) If the applicant is an organisation, the Information Commissioner must send to it, and to other persons (if any) who are interested in the application, a written invitation to notify the Information Commissioner, within the period specified in the invitation, whether or not they wish the Information Commissioner to hold a conference about the draft authorization.

(3) An invitation under subsection (2) shall specify a period that begins on the day on which the invitation is sent and is not shorter than the prescribed period.

6. Conference

(1) If a data controller, or any other interested organisation, or person notifies the Information Commissioner, within the period specified in an invitation sent under paragraph 5, that they wish a conference to be held about the draft authorization, the Information Commissioner shall hold such a conference.

(2) The Information Commissioner shall fix a day, time and place for the holding of the conference.

(3) The day fixed shall not be more than 30 days after the latest day on which a period specified in any of the invitations sent in relation to the draft authorization expires.

(4) The Information Commissioner shall give notice of the day, time and place of the conference to each party to whom an invitation was sent.

7. Conduct of the conference

(1) At the conference, a person to whom an invitation was sent, or any other person who is interested in the application and whose presence at the conference is considered by the Information Commissioner to be appropriate, is entitled to attend and participate personally or, in the case of an organisation, to be represented by a person who is, or persons each of whom is, a director, officer, employee of the organisation.

(2) The Commissioner may exclude from the conference a person who:
(a) is entitled neither to participate in the conference nor to represent a person who is entitled to be represented at the conference;
(b) uses insulting language at the conference;
(c) creates, or takes part in creating or continuing, a disturbance at the conference; or
(d) repeatedly disturbs the conference.

8. Assessment of the application

(1) The Information Commissioner shall, after complying with Part I in relation to the application, make:
(a) such an authorization under paragraph 2 as he or she considers appropriate; or
(b) a written statement dismissing the application. This dismissal shall be considered as final as to the particular processing assessed in the application under specific consideration.

9. Making an authorization

(1) The Information Commissioner shall, in making an authorization, take account of all matters raised at the conference.

(2) The Information Commissioner shall, in making an authorization, take account of all submissions about the application that have been made, whether at a conference or not, by the applicant or any other person or interested party.

Part II—Register of authorizations

1. Register of authorizations

(1) The Information Commissioner must keep a register of authorizations made under Part 1.

(2) The Information Commissioner may decide the form of the register and how it is to be kept.

(3) The Information Commissioner must make the register available to the public in the way

that the Information Commissioner determines.

(4) The Information Commissioner may charge fees for:

(a) making the register available to the public; or
(b) providing copies of, or extracts from, the register.

In Australia, data controllers applying for PIDs are broadly required to provide:

- A detailed and precise description of their intended processing activities;
- Why non-compliance with the relevant legislative or code of practice provision is necessary;
- '[Detailed] arguments demonstrating why the public interest in doing the act or practice outweighs, to a substantial degree, the public interest in adhering to the identified APP or APP code provision';[878] and
- '[Alternative courses of action that have been considered that would not lead to a breach of an APP or registered APP code, with explanations as to why such alternatives are not feasible'.[879]

Although my draft Schedule largely tracks the Australian legislation and the requirements for PIDs, there are important distinctions I would make. First, it is important to distinguish the role of the PIDs under Australian law from the public interest conditions under the DPA 1998. In the UK, the legislative provision for authorization would need to account for the fact that 1) the processing of personal data based on the public interest conditions is *not* considered a breach of data protection law and 2) nor does it provide an exemption from any of a data controller's other obligations under the DPA 1998. The public interest conditions simply satisfy a data controller's obligation to process data lawfully, in line with the first data protection principle in Schedule 1. Second, I would assert a further four distinctions as to what data controllers in the UK would be required to explain when applying for authorization.

1. **A detailed and precise description of their intended processing activities *and its potential effect on the relevant publics.***

   This differs from the Australian PID procedure to incorporate the first key component of the public interest I suggested in Section 3 above (*What public or publics does the data processing in question relate to, and/or who may be affected by this processing?*). Data controllers must describe their processing and specifically account for any effects on 1) the individuals which are indirectly or directly

[878] 'APP' refers to an 'Australian Privacy Principle'. Australian Government Office of the Australian Information Commissioner, 'Privacy Public Interest Determination Guide' (2014) <https://www.oaic.gov.au/agencies-and-organisations/guides/privacy-pid-guide#what-is-pid>.
[879] ibid.

implicated by the dataset(s) *and* 2) any other individuals, groups or publics that may be indirectly or directly affected by the processing in question.

2. **Why their processing is *necessary*.**

   This is like the Australian PID requirement above where alternative courses of action must be considered. In the UK, this requirement would reflect that 1) the public interest conditions do not exempt data controllers from any of their other obligations under the DPA 1998; and 2) reliance on the public interest conditions still hinges on the use of personal data being *necessary* (i.e. the purpose for processing must not be capable of being satisfied by other means, including by using anonymised data).

3. **The extent to which they have *engaged with their data subjects and relevant publics* on this use of data, the results of these engagements and how these have been incorporated into decisions taken. If no engagement activities have been undertaken, a detailed explanation as to why this is not possible.**

   This incorporates the Australian procedure for pre-authorization 'conferences' which allow interested parties to put forward questions and concerns regarding the proposed processing. This also incorporates my suggested, second key component of the public interest: *What are the reasonable expectations of the relevant public/publics as to uses of their data and how will these expectations be translated into the governance of those data?* Here, data controllers must demonstrate their efforts to engage with publics on the proposed use of data and how these views are accounted for in decision-making. The conference procedure in para 6 of the Schedule supports this engagement, while not precluding the broader engagements suggested in the key components and public interest checklist.

4. **Detailed arguments demonstrating why the public interest in their proposed processing outweighs the public and private interests in protecting informational privacy and any other public interests against processing.**

   This is consistent with the Australian procedure and reflects what I propose to be the normative justification underlying my reformulation of the public interest conditions: that the public interest in processing must *outweigh* any negative effect to the public and private interests in protecting informational privacy and any other interests against processing. I have removed the qualifier 'substantially' outweighs considering the procedure authorises the processing of *ordinary* personal data. If it were extended to sensitive personal data, it may be appropriate to include 'substantially'.

5.2.2 Authorization by the ICO

The ICO would play a central role in this authorization scheme. Where applications for authorization are sought (or potentially required for particularly risky, novel or pervasive data processing initiatives) this would shift the burden of determining the appropriate legal basis from a data controller to the ICO, at least in context of processing that would be justifiable based on the public interest conditions. The ICO would be required to:

- Develop the guidance detailing: the circumstances in which applications may be made or where it may be required, the application procedure, format and assessment process (the application could be populated from content similar to what is suggested for the code of practice in Section 4.1 above);
- Be available for initial consultations with data controllers to discuss whether it is 'appropriate' to apply for an authorization (per paragraph 1 of the Schedule);
- Administer the applications process from initial consultation with data controllers, to receipt of the application, to making the authorization or dismissing the application;
- Facilitate public scrutiny of the application process through the mandated 'conference' procedure (per paragraph 6 in the Schedule); and
- Manage a register of applications received and dismissed, and authorizations made (per Part II of the Schedule).

Undoubtedly this is a resource intensive procedure for the ICO to administer, and potentially burdensome for data controllers. However, if authorization is not mandatory for processing relying on the public interest conditions, and indeed is only suggested for exceptionally risky, novel, pervasive or unexpected cases (as discussed above) this would provide legal certainty to data controllers, and security and confidence where it is needed most. As to data controllers, if this were not mandatory but optional, then whether to seek ICO authorization would simply be another factor in their overall risk assessment of the processing in question. And as to the resource implications for the ICO, I would argue that considering their already extensive interactions with the data controller community in the UK, they are best placed to effectively implement this. Moreover, as a body of decisions starts to build, this in itself will provide clarity and guidance as to future processing, which will benefit data controllers and reduce the costs of compliance.

A crucial aspect of the procedure and the ICO's role in it, is the initial consultation with data controllers to assess their suitability for authorization. This would allow the ICO to further guide a data controller's assessment of the public interest and indeed if the public interest conditions apply to the circumstances. Paragraph 3(2)(b) of the Schedule would allow the Commissioner to dismiss applications for several reasons, including if he or she considers the application frivolous, vexatious, misconceived, lacking in substance, or not made in good faith. For these reasons, the procedure should filter out applications which are not likely to satisfy the public interest conditions.

After assessing applications, the ICO would refer to the requirements of the public interest conditions. This would include my suggested legislative changes from Section 4, including the privileging of informational privacy and introducing a mixed test of reasonable belief. Upon determining that a data controller met these requirements, the Information Commissioner would need to approve that the public interest in the proposed use of data *outweighs* the public and private interests in protecting informational privacy and any other counter public interest.

It is this final 'stamp of approval' – that the processing is indeed justifiable in the public interest – that would be most helpful to improving the uncertainty surrounding particularly complex applications of the public interest conditions (e.g. where data processing is novel, pervasive, unexpected etc.). A data controller's hesitancy to rely on the public interest conditions without assistance or supervision, and the (justifiable?) suspicion cast over such opaque decision-making, would be minimised by the creation of this alternative procedure and the role of an independent body to scrutinise these decisions.

5.2.3 Judicial review of the ICO's authorization

Given the detailed nature of the procedure suggested here, courts would have a substantial body of evidence to consider if a legal complaint was lodged against a data controller in receipt of an authorization. I suggest that a *presumption* of legal compliance (with at least the first data protection principle of the DPA 1998) should attach to the

proposed authorization procedure. Unlike the code of practice suggested in Section 5.1 above, the ICO's authorization of a data controller's decision to process data based on the public interest conditions reflects a level of regulatory and public scrutiny that can more legitimately presume legal compliance.

5.2.4 Benefits of administrative authorization of public interest determinations

The authorization of a data controller's decision to process personal data based on the public interest conditions would enhance legal certainty, improve transparency and offer meaningful opportunity for public scrutiny that is currently unavailable under the DPA 1998. The detailed and explicit nature of the procedure would introduce a level of objectivity and consistency to a decision that is inherently context sensitive and normative. Even though authorization may only apply to particularly risky or complex data initiatives, offering this type of procedure would instil confidence in data controllers by removing the perceived risk of taking processing decisions based on the public interest conditions. To satisfy the *normative* dimension of the public interest, this authorization process could further support reliance on the public interest conditions that stays true to the new conceptual understanding offered in this thesis.

The authorization procedure would make data controllers more accountable under the law and to their data subjects and relevant publics, given the transparency of measures provided for. This is particularly important in the complex and pervasive processing circumstances that have been discussed as potentially requiring authorization. In such circumstances data subjects could be informed about the 'how', 'when' and 'why' of processing that is justified based on the 'public interest'. The mandated register of applications would introduce a further level of transparency and could engender trust with relevant publics. The 'conference' procedure would allow relevant publics to intervene and scrutinise public interest justifications *prior* to processing taking place.

Crucial to either of the procedures suggested, is an active ICO. In Section 6 I suggest specific ways in which the ICO can secure the implementation of the public interest

conditions through additions to its already robust approach to engagement with data controllers.

6. Supporting the New Approach to Public Interest Determinations in Data Protection: The Crucial Role of the ICO

In this chapter I have suggested four key components to redeveloping our understanding of the public interest in data protection. To assist data controllers with the assessment of the public interest in their processing, I translated these components into a public interest checklist to guide them through the relevant considerations. To further implement this new understanding I have suggested changes to the legislation and two alternative procedures for deploying the public interest conditions. However, as addressed in Chapter 2, the problem is not only with the law, but also with the culture of caution surrounding the use and sharing of personal data, perpetuated in part by legal uncertainties. To initiate cultural change, data controllers must become confident in their own abilities to meet the requirements of data protection law and better understand the full range of rights and interests that are at stake when they process data. Below I suggest two ways in which the ICO can play a crucial role in addressing these cultures of caution through its engagement and guidance publication scheme.

6.1 The importance of legal myth busting

The literature illustrates a landscape which is dominated by a culture of caution where the mantra is to consent or anonymise all uses of personal data.[880] From this we can deduce that public authorities (and potentially other data controllers) are working under several misconceptions about: 1) the purpose of data protection law; 2) the hierarchy between different processing conditions, and 3) the relative security in anonymisation.

[880] See Chapter 2 Section 2.

The proposed legal and procedural changes could only partially resolve these misconceptions. Legal amendments are not in themselves capable of instilling confidence in data controllers. The ICO already plays a vital role in enforcing data protection law in the UK and in promoting best practice in line with the aims of the legislation. From its informal engagement to its more official enforcement activities, the ICO guides data controllers on the contours of data protection law. What is required is a clear and distinct programme of engagement activity that is focused on *legal myth busting*, catered to specific applications of the law within particular sectors.

Through this programme of engagement, the ICO would be able 'set the record straight' and be clear about what data protection law is and is not within a sphere of activity. The content of such engagement could be developed for a particular data controller audience. From my own experience in engaging with public authorities in the UK, this audience would benefit from clear messages and myth busting around the role and limits of consent and anonymisation as well as on the purpose of data protection law. The ICO could explain within the particular context, how and why data controllers might consider their legal and ethical duties *outside* the consent or anonymisation box; e.g. if the public interest condition is a viable legal basis for processing or if other conditions are relevant to consider. More broadly, the ICO could continue to relay the protective *and* facilitative aims of data protection law, the latter which are frequently forgotten.

6.2 Principles and best practices in new ICO guidance

If data controllers were provided with a clearer understanding of the purpose of data protection law, and the role and relationship between various provisions within it, they would be better equipped and more confident to conceive of their obligations beyond the perceived safety of the consent-or-anonymise paradigm. Data controllers typically lack the tools to engage with the public interest concept in a consistent and objective manner and this can be addressed in the development of new guidance by the ICO. From the freedom of information context, we know that even if the public interest cannot be defined in a final sense, certain principles can be generalised and that more specific guidance can be drawn from a particular context. The ICO is uniquely placed

to derive these principles and more context specific best practice examples, drawing from its rich and varied experiences of engagement with data controllers.

On the ICO website, it already provides guidance on the conditions for processing and explains the meaning of 'necessary' which is part of the public interest conditions.[881] To this, they could add examples of when a data controller might justifiably rely on the public interest conditions. Under the current law, this would reference its guidance on the meaning of 'necessary' but would additionally require defining 'functions of a public nature' and the 'public interest' (and 'substantial' public interest as to sensitive personal data). Here it would also be appropriate to reference the standard by which a data controller's reliance on the public interest conditions would be assessed, i.e. under a mixed test of reasonable belief as suggested in Section 4.2 above. More nuanced advice could be given in sector-specific guides that covered how different types of data controllers and processing activities might rely upon the public interest conditions.

In the context of processing personal or de-identified data for research, there currently is no dedicated guidance, but this is an area which suffers acutely from the culture of caution and legal uncertainty.[882] In guidance tailored to the context of research, the ICO could direct data controllers to different legal bases depending on the purpose of research and how such processing would occur.

More broadly, depending on the purposes for processing (e.g. for improving public service delivery) the ICO could explain relevant and non-relevant factors for data controllers to consider their reliance on the public interest conditions, as opposed to other legal bases for processing. This follows the model of the ICO and SIC guidance on the public interest test in freedom of information law. As to the public interest conditions, relevant factors could include the key components and public interest checklist presented above. This could be complemented by specific case studies of 'successful' and non-successful reliance on the public interest conditions. Overall, such

[881] ICO, 'The Conditions for Processing' (n 159).
[882] See Chapter 2 Section 4.

guidance would breakdown the currently ambiguous task of data controllers independently assessing the public interest in their processing.

7. Improving the Status Quo for the Benefit of Individuals and Data Controllers

The new approach to the public interest suggested in this chapter can improve the way in which data controllers currently conceive of their obligations under data protection law for their benefit and for data subjects.

What I suggest as the key components of the public interest specifically avoid the conceptual vulnerabilities of the concept, and the ambiguity that casts its deployment with suspicion. The emphasis on meaningful public engagement, the importance of legitimate procedures, and the multiplicity of the concept could appropriately reshape what is understood as 'justifiable' reliance on the public interest in different data processing contexts. My suggested procedural approach opens data controller reasoning to public scrutiny, forming a crucial component to deriving *legitimate* determinations on the public interest.

Data controllers derive specific benefits from the approach developed here by enhancements to legal certainty and foreseeability. By privileging the protection of informational privacy within the legislation, data controllers would have a clear and unambiguous steer on the normative weighting to assign in their application of the public interest conditions. And by introducing a standard for assessing their reliance on the public interest conditions, data controllers would know *before* processing data how their decisions could be reviewed – based on a mixed test of reasonable belief. The creation of specific guidance on the public interest conditions, including a 'checklist' of key questions with relevant and typically non-dispositive factors, could better direct data controllers on the ways in which they can responsibly take processing decisions.

Most importantly, however, the legal changes and procedures suggested offer a necessary alternative to the predominant paradigm of compliance based on consent or anonymisation. Throughout this thesis I have argued that neither consent nor anonymisation on its own is capable of fully attending to either the public interest in the protection of individuals' informational privacy or the public interest in certain uses of data. Only by privileging the protection of informational privacy in a legal reformulation of the public interest conditions, could we ensure that its protection is understood for its *public* interest, as opposed to only its private interest value. This could be further secured through the authorization process suggested above and reinforced in a code of practice or authoritative guidance by the ICO. Crucially, within all the legal and procedural suggestions I have made, data controllers would not only have to mitigate risks to informational privacy, they would have to articulate how the potential public interests served by processing *outweigh* any impact presenting the normative justification for using personal data based on the public interest.

Underpinning the approach suggested in this chapter is an active ICO. Even with the uncertainty cast by Brexit, the GDPR will come into force for a period in 2018. This fact and any subsequent post-Brexit interpretation of this legislation will require a strong and proactive approach to enforcement and guidance by the ICO. The suggestions made in this chapter are in keeping with the ICO's current remit and important role it must play in distilling legal guidance against a build-up of socioeconomic and political changes in the UK, Europe and across the globe.

Chapter 7 The Meaning, Value and Utility of the Public Interest Concept for Data Protection Law

1.Future challenges

To bring together the legal and theoretical analysis of this thesis, it is helpful to consider briefly what effect the forthcoming GDPR may have on the issues and potential solutions raised. A comprehensive examination of the impact of the GDPR is beyond the scope of this thesis but my initial analysis indicates that the issues I have identified are not only left unresolved but will potentially worsen under the new Regulation.

The legal grounds for processing in the GDPR are essentially the same as under the current legislation. This means that research may be justified based on consent, the legitimate interests of the data controller or the public interest provision.[883] Critically, however, where a UK university is the data controller, it may no longer be able to rely on the legitimate interests provision, as Article 6(1)(f) prohibits this: 'Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks' (universities being 'public authorities' within the UK and 'research' arguably being an implicit if it not explicit task within their remit).[884] As to consent, it will be increasingly difficult to obtain *valid* consent under the GDPR, especially in the research context, given the specificity required and the impact of rights to withdrawal of consent.[885]

Regarding the 'public interest' provision, the scope of Art 6(1)(e) remains inadequately defined as it has again been left to Member States to determine how the provisions are applied in practice within their jurisdiction, so long as they 'meet an objective of public interest and be proportionate to the legitimate aim pursued'.[886] There still lacks 1) any

[883] GDPR, Art 6(1)(a), (e).
[884] It is unclear whether this was an unintentional result from the narrowing of the legitimate interests provision.
[885] GDPR, Art 7.
[886] GDPR, Recital 45 and Article 6(3).

criteria which data controllers can routinely apply when relying upon the public interest provision or 2) a transparent procedure for making public interest determinations that would be subject to appropriate public (and potentially legal) scrutiny. Thus, while it will be increasingly more difficult to obtain valid consent or to sufficiently anonymise data (given the expanded definition of personal data)[887], the alternatives, such as those based on the public interest, remain *without* sufficient guidance for data controllers to apply in practice.

It follows that the issues identified in this thesis and proposed solutions will remain relevant to the UK post-2018 when the GDPR will come into force. This is so even when considering the uncertain implications of Brexit. It is entirely unclear the extent to which UK data protection legislation will diverge from the GDPR post-Brexit. And moreover, it is unlikely that the UK's withdrawal from the EU will be negotiated and unanimously agreed in less than the two-year period stipulated by Article 50 of the Lisbon treaty. Thus, the GDPR will apply in the UK on 25th May 2018 as it will in all other EU Member States.

2. The Contribution of This Thesis

In this thesis, I sought to examine: under what conditions *can* an individual or organisation justify its processing of personal data based on the public interest, and how is this to be assessed within data protection law? This required an understanding of what the concept means and how it can be more successfully deployed by data controllers in the first instance, and when their decisions are later reviewed by the ICO and courts.

The problematic status quo

In Chapter 2, I stressed the need for developing a better understanding of the public interest conditions. The consent-or-anonymise paradigm was critically evaluated as detrimental to both the protective and facilitative aims of data protection law. Not only does the consent-or-anonymise paradigm neglect the broader public interests in

[887] GDPR, Recital 26.

protecting informational privacy, on a technical level, neither consent nor anonymisation can sufficiently ensure data subjects' rights and interests in their data are respected. The emphasis on either anonymising data prior to use or obtaining consent for 'consent's sake' also negatively impacts the undertaking of publicly beneficial research. In the social sciences and humanities, the consent-or-anonymise paradigm means that certain forms of research may be abandoned if not fundamentally altered to meet the perceived requirements of consent or anonymisation.

To derive a viable public interest alternative to consent or anonymisation, the legal analysis in Chapter 3 provided novel insight into the intended role and scope of the public interest provisions in the DPD. Investigation of the *travaux préparatoires* to the DPD revealed that the public interest concept was included to secure various 'important' forms of processing, including research. The *travaux* demonstrated the lack of any 'hierarchy' between the different legal grounds for processing; consent was one of several alternatives and thus the public interest provisions were not mere 'exceptions' to consent. In this sense, the examination of the *travaux* was critical to establishing the intended *role* of the public interest conditions as translated into the UK's DPA 1998. However, the *travaux* was unable to provide any indication of how data controllers, in the first instance, could assess the public interest in their processing.

The way in which the public interest provisions evolved during the drafting of the DPD demonstrated the utter lack of objectivity or rationales used to assess whether a type of processing was in the public interest. The result was a purely descriptive understanding of the concept, seen in the public interest examples in Recital 34 of the DPD. These examples were added simply because of the lobbying efforts of Member States. EU legislators intended for the public interest provisions to be further elucidated by Member States when introducing their implementing data protection legislation. However, as we saw from the legislative history to the DPA 1998 and the legislation itself, the public interest conditions remained as ambiguous as in the DPD.

Towards a new understanding of the public interest in data protection

In Chapter 4, I expanded this legal analysis to the Article 8 context to consider whether Article 8 jurisprudence in the ECtHR could further substantiate how the public interest in processing should be assessed. The review of Article 8 cases demonstrated the way in which certain procedural principles should apply to public interest determinations, namely, legality, necessity and proportionality. However, the ECtHR's application of these principles was inherently driven by context just as its consideration of the public interest ('legitimate aim' in Article 8).

With only a descriptive and procedural understanding of the public interest, I continued Chapter 4 by looking to theory to derive a fuller and substantive understanding of what the concept can reasonably mean in the context of data protection. Theory revealed the key vulnerabilities of concept, and in turn, what would be required to *normatively* justify the processing of personal data based on the public interest.

To further test this developing conceptual knowledge on the public interest, and to expand our understanding of what is required to successfully deploy the concept, in Chapter 5, I examined the operation of the public interest in cognate areas of law. In evaluating the use of the public interest in freedom of information, copyright and whistleblowing, both generalisable and distinguishing features of the public interest concept were highlighted. Despite the inherent context-sensitive nature of the public interest, where the public interest is deployed, it *is* possible to derive guiding principles on its operation in different contexts. This guidance is crucial where the public interest plays an action-promoting function within legislation, as opposed to a narrower defence or exemption. Such guidance should include the provision of the standard upon which public interest determinations will be assessed.

The value of the public interest to data protection law and practice

Based on the foregoing legal and theoretical analysis, in Chapter 6, I proposed four components to understanding the public interest in data protection:

1. **What public or publics does the data processing in question relate to, and/or who may be affected by this processing?**
2. **What are the reasonable expectations of the relevant public/publics as to uses of their data and how will these expectations be translated into the governance of those data?**
3. **To be justifiable, a data controller's reliance on the public interest to process personal data must be based on the objective consideration of the impact of processing and this must be transparently documented and articulated to the relevant publics.**
4. **The public interest is multiple.**

Crucially, these components avoid the vulnerabilities highlighted by the examination of contested public interest theories and thus overcome the current difficulties in applying the concept to the processing of personal data. They can be used to reshape what is normatively understood as 'justifiable' reliance on the public interest in different data processing contexts. And moreover, the components as translated into my public interest checklist, offer data controllers a way to assess the public interest in their processing where currently they lack any meaningful way of doing so.

To support this reconceptualisation of the public interest in data protection, I proposed crucial amendments to the DPA 1998's public interest conditions. First, to rely on the conditions, data controllers would need to demonstrate that the public interest in their processing of personal data *outweighs* the public (and private) interests in protecting informational privacy (and any other public interests at stake). This could correct the fundamental and damaging misperception that the protection of informational privacy is only a *private* as opposed to a public interest. It more clearly directs data controllers to an objective consideration of whether to base their processing on the public interest conditions, and settles the normative dimension of the public interest consideration. Second, I proposed the introduction of a mixed test of reasonable belief. Introducing an explicit standard for assessing a data controller's initial determination that its processing is 'in the public interest', would 1) enhance legal certainty on the scope of the provisions 2) provide transparency on how these determinations are made in the first instance and 3) demonstrate how reliance on the conditions would be assessed in the regulatory and adjudicative context.

Implementing this reconceptualisation of the public interest and the revised legislative provisions also requires clear and agreed procedures. To this end, I suggested two alternative procedures for making public interest determinations. I first proposed that the ICO should develop a code of practice on how to apply the public interest conditions, with my proposed key components and public interest checklist as practical examples of what this code should contain. The ICO has the knowledge base to derive both principles and context-specific examples for this code of practice from its already extensive engagement efforts with the UK data controller community. The comprehensive guidance already provided on the public interest test in context of freedom of information law, and even on the public interest and reasonable belief standard under section 32 of the DPA 1998, demonstrates the practical feasibility of this option. A code of practice containing practical tools akin to my public interest checklist would offer data controllers a clear method for objectively and consistently assessing the public interest in their processing, and thus whether the public interest conditions apply to their circumstances. By allowing substantiated 'compliance' with the code of practice to serve as evidence of the lawfulness of processing, data controllers would be incentivised to routinely scrutinise the relevant public and private interests at stake in their processing.

The second procedure I suggested was based on the successful operation of a 'public interest determination' scheme in Australia. In the UK, I proposed that the ICO could give prior authorization of a data controller's reliance on the public interest conditions as the legal basis for processing in certain processing circumstances, to be determined potentially by the risks posed by processing. Given the integral role of the conditions for processing and the lack of guidance or interpretation on the deployment of the public interest conditions, I recommended a detailed formulation of a similar procedure to be added as a Schedule to the DPA 1998. Although resource intensive to the ICO, the benefits to operating such a scheme outweigh these costs – not least because of the potential impact of the forthcoming GDPR and thus the more frequent consideration of the public interest conditions by data controllers. For particularly novel, pervasive, unexpected and/or risky forms of processing, authorization would be beneficial from the perspective of uncertain data controllers as well as data subjects who stand to be affected by the processing in question.

The introduction of an authorization procedure in such circumstances could introduce objectivity and consistency to the currently ambiguous scope of the public interest conditions. It could instil *confidence* in data controllers by offering the opportunity for specific consultation and potentially authorization on their decisions to process personal data based on the public interest. The public scrutiny measures within my suggested procedure, including the suggested 'conference' and 'register of authorizations' would ensure that the views of relevant publics are accounted for *prior to* any use of data based on the public interest conditions.

Overall, the new understanding of the public interest offered in this thesis can more fully attend to the interests at the core of data protection – in the protection of informational privacy and in the use of personal data – and ensure they are accounted for in practice. The hope is that these proposals liberate the research community from the uncertainties surrounding data protection law and enable a wide range of publicly beneficial research to be carried out on a solid legal footing – for the benefit of all of us, and for future generations.

Bibliography

Statutes

United Kingdom

Care Act 2014

Copyright, Designs and Patents Act 1988

Data Protection Act 1998

Data Protection Act 1984

Data Protection (Processing of Sensitive Personal Data) Order 2000 S.I. 417

Employment Rights Act 1996

Enterprise and Regulatory Reform Act 2013

Freedom of Information (Scotland) Act 2002

Freedom of Information Act 2000

Human Rights Act 1998

Northern Ireland Act 1998

Public Interest Disclosure Act 1998

Scotland Act 1998

European Union

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281 (Data Protection Directive)

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)

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 (Information Society Directive)

Germany

Federal Data Protection Act (*Bundesdatenschutzgesetz*) 2003

Australia

The Privacy Act 1988 (Commonwealth)

Privacy and Data Protection Act 2014 (Victoria)

Privacy and Personal Information Act 1998 (New South Wales)

Cases

United Kingdom

ALM Medical Services Ltd v Bladon [2002] EWCA Civ 1085, [2002] Emp LR 1054

Ashdown v Telegraph Group Ltd [2001] EWHC Ch 28

Ashdown v Telegraph Group Ltd [2001] EMLR 44

Babula v Waltham Forest College [2007] EWCA Civ 174

Beloff v Pressdram [1973] 1 All ER 241

Cabinet Office and Christopher Lamb v Information Commissioner EA/2008/0024 AND EA/2008/0029 [2009]

Cavendish Munro Professional Risks Management Ltd v Geduld [2010] IRLR 38 (EAT)

Chesterton Global Ltd (t/a Chestertons) and another v Nurmohamed [2015] UKEAT

Chief Constable of West Yorkshire Police v Homer [2012] UKSC 15, [2012] 3 All ER 1287, [2012] ICR 704

Christopher Martin Hogan and Oxford City Council v Information Commissioner ('Hogan') EA20050026 and 0030 [2006]

Corporate Officer of the House of Commons v The Information Commissioner and Others [2009] 3 All ER 403

Farrand v Information Commissioner and another [2014] UKUT 310 (AAC)

Fraser v Evans [1969] 1 QB 349

Gartside v Outram [1857] 26 Ch 113

HP Bulmer Ltd v J Bollinger SA [1974] EWCA Civ 14, [1974] Ch 401 [426]

House of Commons v Information Commissioner and Leapman, Brooke, and Thomas (EA/2007/0060, 26 February 2008)

HRH The Prince of Wales v Associated Newspapers Ltd [2006] EWHC 522 Ch

Hyde Park Residence Ltd v Yelland and others [1999] EWHC Patents 247

Hyde Park Residence Ltd v Yelland [2000] 3 WLR 215

Initial Services Limited v Putterill [1968] 1 QB 396

Johnson v Medical Defence Union (No 1) [2007] EWCA Civ 262

Lion Laboratories Ltd v Evans [1985] QB 526

Mosley v News Group Newspapers Ltd [2008] EWHC 1777 (QB) [138]

Naomi Campbell v Mirror Group Newspapers [2002] EWCA Civ No: 1373

Naomi Campbell v Mirror Group Newspapers [2002] EWHC 499 (QB)

Parkins v Sodexho Ltd [2002] IRLR 109 (EAT)

Pepper v Hart [1992] UKHL 3, [1993] 1 All ER 42 [64]

R (AB) v Chief Constable of Hampshire Constabulary [2015] EWHC 1238 (Admin)

R (Ellis) v Chief Constable of Essex Police [2003] EWHC 1321 (Admin)

R (on the application of Catt) (AP) (Respondent) v Commissioner of Police of the Metropolis and another (Appellants) [2015] UKSC 9

R (Westminster CC) v NASS [2002] UKHL 38

R v Department of Health, ex p Source Informatics Ltd [2000] 1 All ER 786

R v Secretary of State for Employment, ex parte Seymour-Smith (No 2) [2000] 1 All ER 857, [2000] IRLR 263, [2000] 1 WLR 435

R v Secretary of State for the Home Department (ex parte Daly) [2001] UKHL 26

South Lanarkshire Council v Scottish Information Commissioner [2013] UKSC 55

Stone v South East Coast Strategic Health Authority [2006] EWHC 1668 (Admin)

The Christian Institute and others (Appellants) v The Lord Advocate (Respondent) (Scotland) [2016] UKSC 51

YL v Birmingham City Council [2007] UKHL 27

Court of Justice of the European Union

Case C‑201/14 Bara and Others [2015]

Cases C-446/12 and C-449/12 Willems and others [2015]

European Court of Human Rights

Crémieux v France (1993) Series A no 256-B

Dalea v France App no 58243/00 (ECtHR, 1 July 2008)

Dudgeon v The United Kingdom App no 7525/26 (ECtHR, 22 October 1981)

Evans v the United Kingdom App no 6339/05 (ECtHR, 10 April 2007)

Funke v France (1993) Series A no 256-A

Gillow v the United Kingdom (1986) Series A no 109

Handyside v the United Kingdom (1976) Series A no 24

Huber v Bundesrepublik Deutschland C-524/06 (2008) ECR I-9705

Kennedy v The United Kingdom App no 26839/05 (ECtHR, 18 May 2010)

Klass and Others versus Germany App no 5029/71 (ECtHR, 6 September 1978)

Leander v Sweden (1987) Series A no 116

LH v Latvia App No 52019/07 (ECtHR, 29 July 2014)

Liberty and Others v The United Kingdom App no 58243/00 (ECtHR, 1 July 2008)

Malone v the United Kingdom App no 8691/79 (ECtHR, 2 August 1984)

Miailhe v France (1993) Series A no 256-C

Modinos v Cyprus Series A no 259 (ECtHR, 22 April 1993)

Mosley v United Kingdom App no 48009/08 (ECtHR, 12 April 2012)

MS v Sweden (ECtHR 27 August 1997)

Müller And Others v Switzerland Series A no 133 (ECtHR, 24 May 1988)

Nada v Switzerland App no 10593/08 (ECtHR, 12 September 2012)

Norris v Ireland Series A no 142 (ECtHR, 26 October 1988)

Rotaru v Romania App no 28341/95 (ECtHR, 4 May 2000)

S and Marper v The United Kingdom App nos 30562/04 and 30566/04 (ECtHR, 4 December 2008)

Segerstedt-Wiberg and Others v. Sweden App no 62332/00 (ECtHR, 6 June 2006)

SH and Others v Austria App no 57813/00 (ECtHR 3 November 2011)

Silver and Others v the United Kingdom (ECtHR, 25 March 1983)

Sunday Times v The United Kingdom (1979) Series A no 30

Uzun v Germany App no 35623/05 (ECtHR, 2 September 2010)

Australia

O'Sullivan v Farrer (1989) HCA 61

Books

Allen A, 'Genetic Privacy: Emerging Concepts and Values', *Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era* (YUP 1997)

Barocas S and Nissenbaum H, 'Big Data's End Run around Anonymity and Consent' in Julia Lane and others (eds), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (Kindle, CUP 2014)

Barry B, *Political Argument* (Routledge & Kegan Paul 1965)

Benhabib S, 'Toward a Deliberative Model of Democratic Legitimacy' in Seyla Benhabib (ed), *Democracy and difference: Contesting the boundaries of the political* (PUP 1996)

Bennett CJ and Raab C, *The Governance of Privacy: Policy Instruments in Global Perspective* (Ashgate 2002)

Bentham J, *An Introduction to the Principles of Morals and Legislation* (Dover edition, Dove Publications, Inc 2007)

Black G, *Publicity Rights and Image: Exploitation and Legal Control* (Hart Publishing Ltd 2011)

Bowers QC J and others, 'Whistleblowing and Copyright', *Whistleblowing: Law and Practice* (OUP 2012)

Bozeman B, *Public Values and Public Interest: Counterbalancing Economic Individualism* (iTunes Edition, Georgetown University Press 2007)

Buchanan JM and Tullock G, *The Calculus of Consent: Logical Foundations of Constitutional Democracy* (Library of Economics and Liberty 1999)

Burrell R and Coleman A, 'The Public Interest Defence', *Copyright Exceptions: The Digital Impact* (CUP 2005)

Bygrave LA and Schartum DW, 'Consent, Proportionality and Collective Power' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer 2009)

Carter M and Bouris A, *Freedom of Information: Balancing The Public Interest* (Second, The Constitution Unit University College London 2006)

Cassinelli CW, 'The Public Interest in Political Ethics', *Nomos V: The Public Interest* (Atherton Press 1962)

Cavoukian A, 'Evolving FIPPs: Proactive Approaches to Privacy, Not Privacy Paternalism', *Reforming European Data Protection Law* (Springer 2015)

Copinger and Skone James on Copyright (17th edn, Sweet & Maxwell 2016)

Dahl R and Lindblom R, *Politics, Economics and Welfare* (Second, Transaction Publishers 2000)

Davies G, *Copyright and the Public Interest* (2nd edition, Sweet & Maxwell 2002)

Dworkin R, *Taking Rights Seriously* (Bloomsbury Publishing 2013)

Edwards L and Brown I, 'Data Control and Social Networking: Irreconcilable Ideas?' in A Matwyshyn (ed), *Harboring Data: Information Security, Law and the Corporation* (SUP 2009)

El Emam K, *Guide to the De-Identification of Personal Health Information* (CRC Press Taylor & Francis Group 2013)

Faden R, Beauchamp T and King N, *A History and Theory of Informed Consent* (OUP 1986)

Flathman RE, *The Public Interest: An Essay Concerning the Normative Discourse of Politics* (John Wiley & Sons, Inc 1966)

——, *Concepts in Social and Political Philosophy* (Macmillan Publishing Co, Inc 1973)

Friedrich CJ, *Nomos V: The Public Interest* (Atherton Press 1962)

Fuller LL, *The Morality of Law* (Revised Edition, YUP)

Garnett K, 'The Impact of the Human Rights Act 1998 on UK Copyright Law', *Copyright and Free Speech: Comparative and International Analyses* (OUP 2005)

Habermas J, *Between Facts and Norms: Contribution to a Discourse Theory of Law and Democracy* (MIT Press 1996)

Hadfield P, *Bar Wars: Contesting the Night in Contemporary British Cities* (OUP 2006)

Held V, *The Public Interest and Individual Interests* (Basic Books 1970)

——, *Rights and Goods: Justifying Social Action* (2nd edn, University of Chicago Press 1989)

Hobbes T, *Leviathan* (iTunes edition, Public Domain 1679)

Hobbs D and others, *Bouncers: Violence and Governance in the Night-Time Economy* (OUP 2003)

Hume D, *An Enquiry Concerning the Principles of Morals* (Eighteenth Century Collections Online, Gale 2004)

Jay R, *Data Protection Law & Practice* (4th edn, Sweet & Maxwell 2012)

Kosta E, *Consent in European Data Protection Law* (Martinus Nijhoff Publishers 2013)

Laurie G, *Genetic Privacy: A Challenge to Medico-Legal Norms* (CUP 2002)

Lippmann W, *The Phantom Public* (10th edn, Transaction Publishers 2011)

Mansbridge J, 'On the Contested Nature of the Public Good' in Walter W Powell and Elisabeth S Clemens (eds), *Private Action and the Public Good* (YUP 1998)

Manson NC and O'Neill O, *Rethinking Informed Consent in Bioethics:* (CUP 2007)

Miceli MP and Near JP, *Blowing the Whistle: The Organizational and Legal Implications for Companies and Employees* (Lexington Books 1992)

Raab C, 'Privacy, Social Values and the Public Interest', *Politik und die Regulierung von Information* (Nomos verlagsgesellschaft, Baden-Baden 2012)

Rawls J, A Theory of Justice (Harvard University Press 2009).

Regan PM, *Legislating Privacy: Technology, Social Values, and Public Policy* (University of North Carolina Press 1995)

Rousseau J-J, *On The Social Contract* (Drew Silver ed, GDH Cole tr, Dover Publications, Inc 2003)

Schauer F, 'Proportionality and the Question of Weight', *Proportionality and the Rule of Law: Rights, Justification, Reasoning* (CUP 2014)

Schoeman FD, *Privacy and Social Freedom* (1st edn, CUP 1992)

Schubert GA, *The Public Interest: A Critique of the Theory of a Political Concept* (The Free Press 1960)

Solove DJ, *Understanding Privacy* (Kindle Edition, Harvard University Press 2008)

Steeves VM, 'Reclaiming the Social Value of Privacy', *Lessons from the identity trail: anonymity, privacy, and identity in a networked society* (OUP 2009)

Stevens L, Dobbs C, Jones K and Laurie G, 'Dangers from Within? Looking Inwards at the Role of Maladministration as the Leading Cause of Health Data Breaches in the UK', *Data Protection and Privacy: (In)visibilities and Infrastructures* (Springer 2017)

Strandberg KJ, 'Monitoring, Datafication, and Consent: Legal Approaches to Privacy in the Big Data Context', *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (Kindle Edition, CUP 2014)

Taylor M, *Genetic Data and the Law: A Critical Perspective on Privacy Protection* (CUP 2012)

Townend D, 'Overriding Data Subjects' Rights in the Public Interest' in Deryck Beyleveld and others (eds), *The Data Protection Directive and Medical Research Across Europe* (Ashgate 2004)

Walden I, 'Privacy and Data Protection', *Computer Law: The Law and Regulation of Information Technology* (7th edn, OUP 2011)

Weindling P, *Nazi Medicine and the Nuremberg Trials: From Medical Warcrimes to Informed Consent* (Palgrave Macmillan UK 2004)

Widdows H, *The Connected Self* (1st edn, CUP 2013)

Journals

Audrey S and others, 'Young People's Views about Consenting to Data Linkage: Findings from the PEARL Qualitative Study' (2016) 16 BMC Medical Research Methodology 34

Balboni P and others, 'Legitimate Interest of the Data Controller New Data Protection Paradigm: Legitimacy Grounded on Appropriate Protection' (2013) 3 International Data Privacy Law 244

Bamberger KA and Mulligan DK, 'Privacy on the Books and on the Ground' (2010) 63 Stanford Law Review 247

Bellia PL, 'Federalization in Information Privacy Law' (2009) 118 Yale Law Journal 868

Beyleveld D, 'Data Protection and Genetics: Medical Research and the Public Good' (2007) 18 King's Law Journal 275

Black G and Stevens L, 'Enhancing Data Protection and Data Processing in the Public Sector: The Critical Role of Proportionality and the Public Interest' (2013) 10 SCRIPTed 1

boyd danah, Levy K and Marwick A, 'The Networked Nature of Algorithmic Discrimination'

Braybrooke D, 'Review: The Public Interest and Individual Interests. Virginia Held.' (1972) 69 The Journal of Philosophy 192

Brownsword R, 'The Cult of Consent: Fixation and Fallacy' (2004) 15 Kings College Law Journal

Burrell R, 'Defending the Public Interest' (2000) European Intellectual Property Review 394

Callahan ES, Dworkin TM and Lewis D, 'Whistleblowing: Australian, U.K., and U.S. Approaches to Disclosure in the Public Interest' (2004) Virginia Journal of International Law 879

Carter P, Laurie GT and Dixon-Woods M, 'The Social Licence for Research: Why Care.data Ran into Trouble' (2015) Journal of Medical Ethics

Charlesworth A, 'Data Protection, Freedom of Information and Ethical Review Committees' (2012) 15 Information, Communication & Society 85

Cohen JE, 'Examined Lives: Informational Privacy and the Subject as Object' (2000) 52 Stanford Law Review 1373

Connelly R and others, 'The Role of Administrative Data in the Big Data Revolution in Social Science Research' Social Science Research

Corrigan O, 'Empty Ethics: The Problem with Informed Consent' (2003) 25 Sociology of Health & Illness 768

Crawford K and Schultz J, 'Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms' (2014) 55 BCL Rev. 93

Custers B, 'Click Here to Consent Forever: Expiry Dates for Informed Consent' (2016) 3 Big Data & Society

——, 'Informed Consent in Social Media Use. The Gap between User Expectations and EU Personal Data Protection Law' (2013) 10 SCRIPTed 435

Dehon E, 'Divining the Public Interest' (2016) 12 Freedom of Information 8

Dingwall R, 'The Ethical Case against Ethical Regulation in Humanities and Social Science Research' (2008) 3 21st Century Society: Journal of the Academy of Social Sciences 1

Donnelly Catherine, 'Privatization and Welfare: A Comparative Perspective' (2011) 5 Law & Ethics of Human Rights 337

Dove E and Laurie G, 'Consent and Anonymisation: Beware Binary Constructions' (2015) 350 BMJ

Dyer S and Demeritt D, 'Un-Ethical Review? Why It Is Wrong to Apply the Medical Model of Research Governance to Human Geography' (2009) 33 Progress in Human Geography 46

Edwards L, 'Taking the "Personal" Out of Personal Data: Durant v FSA and Its Impact on the Legal Regulation of CCTV' (2004) 1 SCRIPTed 341

El Emam K, Rodgers S and Malin B, 'Anonymising and Sharing Individual Patient Data' (2015) 350 BMJ

Erdos D, 'Stuck in the Thicket? Social Research under the First Data Protection Principle' (2011) 19 International Journal of Law and Information Technology 133

——, 'Systematically Handicapped? Social Research in the Data Protection Framework' (2011) 20 Information and Communications Technology Law 83

——, 'Constructing the Labyrinth: The Impact of Data Protection on the Development of "Ethical" Regulation in Social Science' (2012) 15 Information Communication and Society 104

——, 'Freedom of Expression Turned on Its Head? Academic Social Research and Journalism in the European Union's Privacy Framework' (2013) Public Law 52

Eriksson S, Högland A and Helgesson G, 'Do Ethical Guidelines Give Guidance? A Critical Examination of Eight Ethics Regulations' (2008) 17 Cambridge Quarterly of Healthcare Ethics 15

Fedorowicz J, Gogan JL and Culnan MJ, 'Barriers to Interorganizational Information Sharing in E-Government: A Stakeholder Analysis' (2010) 26 The Information Society 315

Gallie WB, 'Essentially Contested Concepts' (1955) 56 Proceedings of the Aristotelian Society 167

Gauthier D, 'Reason and Maximization' (1975) 4 Canadian Journal of Philosophy 411

Gil-Garcia JR, Chengalur-Smith I and Duchessi P, 'Collaborative E-Government: Impediments and Benefits of Information-Sharing Projects in the Public Sector' (2007) 16 European Journal of Information Systems 121

Gobert J and Punch M, 'Whistleblowers, the Public Interest, and the Public Interest Disclosure Act 1998' (2000) 63 The Modern Law Review 25

Griffiths J, 'Pre-Empting Conflict – a Re-Examination of the Public Interest Defence in UK Copyright Law' (2014) 34 Legal Studies 76

Gymrek M and others, 'Identifying Personal Genomes by Surname Inference' (2013) 339 Science 321

Hedgecoe A, 'Research Ethics Review and the Sociological Research Relationship' (2008) 42 Sociology 873

Held V, 'Rationality and Social Value in Game-Theoretical Analyses' (1966) 76 Ethics 215
——, 'On the Meaning of Trust' (1968) 78 Ethics 156

——, 'Justification: Legal and Political' (1975) 86 Ethics 1

Iversen A and others, 'Consent, Confidentiality, and the Data Protection Act' (2006) 332 BMJ 165

Jones KH and others, 'The Other Side of the Coin: Harm due to the Non-Use of Health-Related Data' (2017) 97 International Journal of Medical Informatics 43

Kent J and others, 'Social Science Gets the Ethics Treatment: Research Governance and Ethical Review' (2002) 7 Sociological Research Online

Laurie G, 'Evidence of Support for Biobanking Practices' (2008) 337 BMJ

Laurie G and Postan E, 'Rhetoric or Reality: What Is the Legal Status of the Consent Form in Health-Related Research?' [2012] Medical Law Review

Laurie G and Stevens L, 'Developing a Public Interest Mandate for the Governance and Use of Administrative Data in the United Kingdom' (2016) 43 Journal of Law and Society 360

Lewis D, 'Ten Years of Public Interest Disclosure Legislation in the UK: Are Whistleblowers Adequately Protected?' (2008) 82 Journal of Business Ethics 497

Lips AMB, O'Neill RR and Eppel EA, 'Cross-Agency Collaboration in New Zealand: An Empirical Study of Information Sharing Practices, Enablers and Barriers in Managing for Shared Social Outcomes' (2011) 34 Int J Public Adm

Margulis ST, 'Privacy as a Social Issue and Behavioral Concept' (2003) 59 Journal of Social Issues 243

McHarg A, 'Reconciling Human Rights and the Public Interest: Conceptual Problems and Doctrinal Uncertainty in the Jurisprudence of the European Court of Human Rights' (1999) 62 Modern Law Review 671

Mitnick BM, 'A Typology of Conceptions of the Public Interest' (1976) 8 Administration & Society 5

Müller JW, 'A General Theory of Constitutional Patriotism' (2008) 6 International Journal of Constitutional Law 72

Murphy E and Dingwall R, 'Informed Consent, Anticipatory Regulation and Ethnographic Practice' (2007) 65 Informed Consent in a Changing Environment 2223

Nissenbaum H, 'A Contextual Approach to Privacy Online' (2011) 140 Daedalus 32

O'Flynn I, 'Deliberating About the Public Interest' (2010) 16 Res Publica 299

Ohm P, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2009) 57 UCLA Law Review 1701

O'Keefe CM and Connolly CJ, 'Privacy and the Use of Health Data for Research' (2010) 193 The Medical Journal of Australia 537

Palmer S, 'Public Functions and Private Services: A Gap in Human Rights Protection' (2008) 6 International Journal of Constitutional Law 585

Peto J, Fletcher O and Gilham C, 'Data Protection, Informed Consent, and Research' (2004) 328 BMJ 1029

Pollock K, 'Procedure versus Process: Ethical Paradigms and the Conduct of Qualitative Research' (2012) 13 BMC Medical Ethics 1

Schwartz PM, 'Privacy and Democracy in Cyberspace' (1999) 52 Vanderbilt Law Review 1607

Schwartz PM, 'Preemption and Privacy' (2009) 118 Yale Law Journal

Schwartz PM and Solove DJ, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information' (2011) 86 New York University Law Review 1814

Sethi N and Laurie G, 'Delivering Proportionate Governance in the Era of eHealth: Making Linkage and Privacy Work Together' (2013) 13 Medical Law International 168

Simm K, 'The Concepts of Common Good and Public Interest: From Plato to Biobanking' (2011) 20 Cambridge Quarterly of Healthcare Ethics 554

Sims A, 'The Denial of Copyright Protection on Public Policy Grounds' (2008) 30 European Intellectual Property Review 189

Solove DJ, 'Privacy Self-Management and the Consent Dilemma' (2013) 126 Harvard Law Review 1880

Sorauf F, 'The Public Interest Reconsidered' (1957) 19 Journal of Politics 616

Stevens L, 'The Proposed Data Protection Regulation and Its Potential Impact on Social Sciences Research in the UK' (2015) 1 European Data Protection Law Review

Strobl J, Cave E and Walley T, 'Data Protection Legislation: Interpretation and Barriers to Research' (2000) 321 BMJ 890

Sweeney L, 'Achieving K-Anonymity Privacy Protection Using Generalization and Suppression' (2002) 10 International Journal on Uncertainty, Fuzziness and Knowledge-based Systems 571

——, 'K-Anonymity: A Model for Protecting Privacy' (2002) 10 International Journal on Uncertainty, Fuzziness and Knowledge-based Systems 557

Sweeney L and Yoo JS, 'De-Anonymizing South Korean Resident Registration Numbers Shared in Prescription Data' (2015) Technology Science

Taylor M, 'Health Research, Data Protection, and the Public Interest in Notification' (2011) 19 Medical Law Review 267

Terry N, 'Big Data Proxies and Health Privacy Exceptionalism' (2014) 24 65

van der Sloot B, 'How to Assess Privacy Violations in the Age of Big Data? Analysing the Three Different Tests Developed by the ECtHR and Adding for a Fourth One' (2015) Information & Communications Technology Law 1

Waldron J, 'Is the Rule of Law an Essentially Contested Concept (In Florida)?' (2002) 21 Law and Philosophy 137

Walley T, 'Using Personal Health Information in Medical Research' (2006) 332 BMJ 130

Warner M, 'Publics and Counterpublics' (2002) 14 Public Culture 49

Wauters E, Lievens E and Valcke P, 'Towards a Better Protection of Social Media Users: A Legal Perspective on the Terms of Use of Social Networking Sites' (2014) 22 International Journal of Law and Information Technology 254

Weindling P, 'The Origins of Informed Consent: The International Scientific Commission on Medical War Crimes, and the Nuremberg Code' (2001) 75 Bulletin of the History of Medicine 37

Wiles R, Crow G, Charles V and Heath S, 'Informed Consent and the Research Process: Following Rules or Striking Balances?' (2007) 12 Sociological Research Online

Wiles R, Crow G, Heath S and Charles V, 'The Management of Confidentiality and Anonymity in Social Research' (2008) 11 International Journal of Social Research Methodology 417

Wiles R, Coffey A, Robinson J and Heath S, 'Anonymisation and Visual Images: Issues of Respect, "voice" and Protection' (2011) 15 International Journal of Social Research Methodology 41

Wiles R, Coffey A, Robinson J and Prosser J, 'Ethical Regulation and Visual Methods: Making Visual Research Impossible or Developing Good Practice?' (2012) 17 Sociological Research Online 8

Williams A, 'YL v Birmingham City Council: Contracting out and "Functions of a Public Nature"' (2008) 4 European Human Rights Law Review 524

Working Papers and Theses

Barocas S and Nissenbaum, Helen, 'On Notice: The Trouble with Notice and Consent' (2009) <https://www.nyu.edu/projects/nissenbaum/papers/ED_SII_On_Notice.pdf>

Black G, 'A Right of Publicity in Scots Law' (2009 University of Edinburgh, Doctoral Thesis)

Laurie G and Harmon S, 'Through the Thicket and Across the Divide: Successfully Navigating the Regulatory Landscape in Life Sciences Research' (2013 University of Edinburgh, School of Law Research Paper No 2013/30)

Laurie G and Sethi N, 'Information Governance Of Use Of Health-Related Data In Medical Research In Scotland: Current Practices And Future Scenarios' (2011) Working Paper No. 1 <http://www.scot-ship.ac.uk/sites/default/files/Reports/Working_Paper_1.pdf>

Laurie G and Stevens L, 'The Administrative Data Research Centre Scotland: A Scoping Report on the Legal & Ethical Issues Arising from Access & Linkage of Administrative Data' (2014 University of Edinburgh, School of Law Research Paper No 2014/35)

Narayanan A and Shmatikov V, 'De-Anonymizing Social Networks', *30th IEEE Symposium on Security & Privacy* (2009) <https://www.cs.utexas.edu/~shmat/shmat_oak09.pdf>

Rauhofer J, 'Round and Round the Garden? Big Data, Small Government and the Balance of Power in the Information Age' (2014 University of Edinburgh, School of Law Research Paper No 2014/06)

Official Publications and Guidance

Article 29 Data Protection Working Party, 'Opinion 7/2003 on the Re-Use of Public Sector Information and the Protection of Personal Data: Striking the Balance' (2003) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2003/wp83_en.pdf>

——, 'Opinion 05/2014 on Anonymisation Techniques' (2014) WP216 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>

European Commission, 'Amended Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data' (1992) OJ C311/30 <http://aei.pitt.edu/10375/1/10375.pdf>

European Parliament, 'Position of the European Parliament on Proposal for a Directive I COM (90) — C3-0323/90 — SYN 287/Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data, 11 March 1992 (First Reading)' (1992) OJ C94/173 <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOC_1992_094_R_0063_01&from=EN>

——, 'A Comparison between US and EU Data Protection Legislation for Law Enforcement' (2015)

<http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU%282015%29536459_EN.pdf>

Financial Conduct Authority, 'Accountability and Whistleblowing Instrument 2015' <https://www.handbook.fca.org.uk/instrument/2015/FCA_2015_46.pdf>
House of Lords, Science and Technology Committee, '2nd Report of Session 2008-09, Genomic Medicine' (2009) <http://www.publications.parliament.uk/pa/ld200809/ldselect/ldsctech/107/107i.pdf>

ICO, 'Data Protection Act 1998 Legal Guidance' (2001)

——, 'Anonymisation: Managing Data Protection Risk Code of Practice' (2012) <https://ico.org.uk/media/1061/anonymisation-code.pdf>

——, 'Data Protection and Journalism: A Guide for the Media' (2014) <https://ico.org.uk/media/1552/data-protection-and-journalism-media-guidance.pdf>

——, 'Processing Personal Data Fairly and Lawfully (Principle 1)' (2016) <https://ico.org.uk/for-organisations/guide-to-data-protection/principle-1-fair-and-lawful/>

——, 'The Conditions for Processing' (2016) <https://ico.org.uk/for-organisations/guide-to-data-protection/conditions-for-processing/>

——, 'The Public Interest Test: Freedom of Information Act' (2016) <https://ico.org.uk/media/for-organisations/documents/1183/the_public_interest_test.pdf>

——, 'When Is Processing Necessary?' <https://ico.org.uk/for-organisations/guide-to-data-protection/conditions-for-processing/>

——, 'The Guide to Data Protection' (2016) <https://ico.org.uk/media/for-organisations/guide-to-data-protection-2-4.pdf>

The Right Honourable Lord Justice Leveson, 'The Leveson Inquiry: An Inquiry Into the Culture, Practices and Ethics of the Press' (2012) Volume 3 <http://webarchive.nationalarchives.gov.uk/20140122145022/http://www.official-documents.gov.uk/document/hc1213/hc07/0780/0780_iii.asp>.

'Legislative Powers: Ordinary Legislative Procedure' (*European Parliament: About Parliament*) <http://www.europarl.europa.eu/aboutparliament/en/20150201PVL00004/Legislative-powers>

Ministry of Justice, 'The Data Sharing Protocol: Annex H, Legal Guidance on Data Sharing' (27 July 2012) <http://www.justice.gov.uk/downloads/information-access-rights/data-sharing/annex-h-data-sharing.pdf>

National Data Guardian, 'Review of Data Security, Consent and Opt-Outs' (2016) <https://www.gov.uk/government/publications/review-of-data-security-consent-and-opt-outs>

NHS, 'Recommendations and Approval Decisions' <http://www.hra.nhs.uk/documents/2014/02/cag-frequently-asked-questions-3.pdf>

'OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data - OECD' (as updated in 2013) <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>

Office of the Australian Information Commissioner AG, 'Privacy Public Interest Determination Guide' (2014) <https://www.oaic.gov.au/agencies-and-organisations/guides/privacy-pid-guide#what-is-pid>

——, 'Public Interest Determinations: Privacy Registers' (2015) <https://www.oaic.gov.au/privacy-law/privacy-registers/public-interest-determinations/>

'Opinion on: — the Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data, — the Proposal for a Council Directive Concerning the Protection of Personal Data and Privacy in the Context of Public Digital Telecommunications Networks, in Particular the Integrated Services Digital Network (ISDN) and Public Digital Mobile Networks, and — the Proposal for a Council Decision in the Field of Information Security' (Economic and Social Committee 1991) C 159/38 <http://publications.europa.eu/resource/cellar/4ed85510-f142-461b-bd0d-fc850f77fbf3.0004.01/DOC_1>

'Oral Evidence' (*UK House of Lords, Science and Technology Committee, 2nd Report of Session 2008-09*, 2009) <www.publications.parliament.uk/pa/ld200809/ldselect/ldsctech/107/107i.pdf>

'Oral Evidence - Responsibilities of the Secretary of State for Culture, Media and Sport' (24 October 2016) <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/culture-media-and-sport-committee/responsibilities-of-the-secretary-of-state-for-culture-media-and-sport/oral/42119.html>

'Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data 1990/C/277/03' <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:1990:277:FULL&from=en>

'Public Interest Directions' (*Information and Privacy Commission New South Wales*, 2016) <http://www.ipc.nsw.gov.au/public-interest-directions>

Scottish Executive, 'Data Sharing: Legal Guidance for the Scottish Public Sector' (2004) <http://www.scotland.gov.uk/Publications/2004/10/20158/45768>

Scottish Information Commissioner, 'Information Intended for Future Publication' <http://www.itspublicknowledge.info/Law/FOISA-EIRsGuidance/section27/Section27.aspx>

——, 'The Public Interest Test in FOISA: Briefing' (2016) <http://www.itspublicknowledge.info/nmsruntime/saveasdialog.aspx?lID=9842&sID=684>

State Government of Victoria C for P and DP, 'Guidelines to Public Interest Determinations, Temporary Public Interest Determinations, Information Usage Arrangements and Certification' (2014) <https://www.cpdp.vic.gov.au/images/content/pdf/Guidelines_to_Public_Interest_Determinations.pdf>

Academic Guidelines

'Code of Practice for Research: Promoting Good Practice and Preventing Misconduct' (UK Research Integrity Office 2009) <http://ukrio.org/wp-content/uploads/UKRIO-Code-of-Practice-for-Research.pdf>

ESRC, 'Data Protection' <http://www.esrc.ac.uk/funding/guidance-for-applicants/research-ethics/frequently-raised-topics/data-requirements/data-protection/>

'ESRC Framework for Research Ethics - Updated January 2015' (2015) <http://www.esrc.ac.uk/_images/framework-for-research-ethics_tcm8-33470.pdf>

JISC, 'Processing Personal Data' (2014) <https://www.jisc.ac.uk/guides/data-protection-and-research-data/processing-personal-data>

'Our Principles: Researchers and Research Teams' (*ESRC*) <http://www.esrc.ac.uk/funding/guidance-for-applicants/research-ethics/our-principles-researchers-and-research-teams/>

RCUK, 'RCUK Policy and Guidelines on Governance of Good Research Conduct' (2015) <http://www.rcuk.ac.uk/documents/reviews/grc/rcukpolicyandguidelinesongovernanceofgoodresearchpracticefebruary2013-pdf/>

'Research Data: Data Protection and Research' (*London School of Economics*, 2016) <http://www.lse.ac.uk/intranet/LSEServices/Legal%20Team/dataProtection/researchData.aspx>

'Researcher's Guide to the Data Protection Principles' (*The University of Edinburgh*, 2015) <http://www.ed.ac.uk/records-management/data-protection/guidance-policies/research-and-the-data-protection-act/research/guide-principles>

'Statement of Ethical Practice for the British Sociological Association (March 2002)' (*British Sociological Association*, 2002) <https://www.britsoc.co.uk/equality-diversity/statement-of-ethical-practice/>

'Subject Coverage' (*Arts and Humanities Research Council*) <http://www.ahrc.ac.uk/funding/research/subjectcoverage/>

'The Concordat to Support Research Integrity' (*Universities UK*, 2012) <http://www.universitiesuk.ac.uk/policy-and-analysis/reports/Pages/research-concordat.aspx>

The University of Edinburgh, 'Research and the Data Protection Act' (2008) <http://www.ed.ac.uk/records-management/data-protection/guidance-policies/research/act>

——, 'Data Protection for Students' (2014) <http://www.ed.ac.uk/records-management/data-protection/guidance-policies/dpforstudents>

——, 'University of Edinburgh Data Protection Policy' (2015) <http://www.ed.ac.uk/records-management/data-protection/data-protection-policy>

——, 'Generation Scotland - General Information' (2016) <http://www.ed.ac.uk/generation-scotland/about/general-information>

——, 'Research Ethics and Data Protection' (2016) <http://www.ed.ac.uk/records-management/data-protection/guidance-policies/research/ethics>

UK Data Archive, 'Consent' (2016) <http://www.data-archive.ac.uk/create-manage/consent-ethics/consent>

Technical Reports

Clark S and Weale A, 'An Analysis of the Social Values Involved in Data Linkage Studies: Information Governance in Health' (Nuffield Trust 2011) <http://www.nuffieldtrust.org.uk/sites/files/nuffield/information_governance_in_health_-_research_report-_aug11.pdf>

Greer S, 'The Exceptions to Articles 8 to 11 of the European Convention on Human Rights' (Council of Europe 1997) <http://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-15(1997).pdf>

Laurie G, Jones K, Stevens L, Dobbs C, 'A Review of Evidence Relating to Harm Resulting from Uses of Health and Biomedical Data' (Nuffield Council on Bioethics

and Wellcome Trust Expert Advisory Group on Data Access 2015) <http://nuffieldbioethics.org/project/biological-health-data/evidence-gathering/>

Laurie G, Stevens L, Longmore B, Hagan H, 'From a Culture of Caution to a Culture of Confidence: Lessons Learned from Implementing the Public Records (Scotland) Act 2011 - Workshop Report' (2016) <http://www.nrscotland.gov.uk/files//record-keeping/public-records-act/prsa-adrc-report.pdf>

Lee YH, Laidlaw E and Mac Síthigh D, 'Copyright and Freedom of Expression: A Literature Review' (2015) <http://www.create.ac.uk/publications/copyright-and-freedom-of-expression-a-literature-review/>

Public Health Research Data Forum, 'Enabling Data Linkage to Maximise the Value of Public Health Research Data' (Wellcome Trust 2015) <https://wellcome.ac.uk/sites/default/files/enabling-data-linkage-to-maximise-value-of-public-health-research-data-phrdf-mar15.pdf>

Rumbold B, Lewis G and Bardsley M, 'Understanding Information Governance: Access to Person-Level Data in Healthcare' (Nuffield Trust 2011) <http://www.nuffieldtrust.org.uk/publications/access-person-level-data-health-care-understanding-information-governance>

Sane J and Edelstein M, 'Overcoming Barriers to Data Sharing in Public Health: A Global Perspective' (Chatham House: The Royal Institute of International Affairs 2015) <https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20150417OvercomingBarriersDataSharingPublicHealthSaneEdelstein.pdf>

The Academy of Medical Sciences, 'Personal Data for Public Good: Using Health Information in Medical Research' (2006) <http://www.acmedsci.ac.uk/download.php?f=file&i=13206>

——, 'A New Pathway for the Regulation and Governance of Health Research' (2011) <http://www.acmedsci.ac.uk/download.php?file=/images/project/130734957423.pdf>

The Law Commission, 'Data Sharing Between Public Bodies - A Scoping Report' (2014) <http://lawcommission.justice.gov.uk/docs/lc351_data-sharing.pdf>

Thomas R and Walport M, 'Data Sharing Review Report' (2008) <http://webarchive.nationalarchives.gov.uk/+/http:/www.justice.gov.uk/docs/data-sharing-review.pdf>

Wiles R, Heath S, Crow G and Charles V, 'Informed Consent in Social Research: A Literature Review' (2005) NCRM 001 ESRC National Centre for Research Methods

Websites

'About Us' (NHS: Health Research Authority) <http://www.hra.nhs.uk/about-the-hra/>

'Action We've Taken' (ICO, 2016) <https://ico.org.uk/action-weve-taken/>

'Administrative Data Research Centre Scotland' <http://adrn.ac.uk/centres/scotland>

ADRN, 'Data Protection Act' <https://adrn.ac.uk/getting-data/resources/legal/>

'Advisory Visits' (ICO, 2016) <https://ico.org.uk/for-organisations/improve-your-practices/advisory-visits/>

'A Leitkultur for Germany - What Exactly Does It Mean?' ((German) Federal Ministry of the Interior, 2017) <http://www.bmi.bund.de/SharedDocs/Interviews/EN/2017/namensartikel-bild.html>

'Annex - Summary of GDPR Derogations in the Data Protection Bill' (2017) <https://webcache.googleusercontent.com/search?q=cache:vmMWzT2gNBkJ:https://www.twobirds.com/~/media/pdfs/summary-of-gdpr-derogations-in-data-protection-bill.pdf%3Fla%3Den+&cd=1&hl=en&ct=clnk&gl=uk&client=safari>

'Article 29 Working Party' (European Data Protection Supervisor) <https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/Art29>

'Audits' (ICO, 2016) <https://ico.org.uk/for-organisations/improve-your-practices/audits/>

Barbaro M and Zeller T, 'A Face Is Exposed for AOL Searcher No. 4417749 - New York Times' <http://www.nytimes.com/2006/08/09/technology/09aol.html?pagewanted=all&_r=0>

'Benefits of Administrative Data' (Administrative Data Research Network, 2016) <https://adrn.ac.uk/getting-data/admin-data/>

Boardman R, Mullock J and Drake E, 'The UK Government Publishes Its Statement of Intent for Data Protection Bill and GDPR' (Bird & Bird) <https://www.twobirds.com/en/news/articles/2017/uk/uk-government-publishes-its-statement-of-intent-for-data-protection-bill-and-gdpr>

Bolten E, 'Care.data Has Been Scrapped, but Your Health Data Could Still Be Shared' <http://theconversation.com/care-data-has-been-scrapped-but-your-health-data-could-still-be-shared-62181>

'Data Security Incident Trends' (ICO, 2 December 2016) <https://ico.org.uk/action-weve-taken/data-security-incident-trends/>

Department for Digital, Culture Media & Sport, 'A New Data Protection Bill: Our Planned Reforms' (2017) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/635900/2017-08-07_DP_Bill_-_Statement_of_Intent.pdf>

'Editorial Guidelines' (BBC, 2016) <http://www.bbc.co.uk/editorialguidelines/guidelines>

'Editors' Code of Practice' (Independent Press Standards Organisation, 2016) <https://www.ipso.co.uk/editors-code-of-practice/>

'EUR-Lex - 1990_287 - EN' (EUR-Lex: Access to European Union law) <http://eur-lex.europa.eu/procedure/EN/100979>

'Europe Claims UK Botched One Third of Data Protection Directive' (Out-law.com: legal news and guidance from Pinsent Masons) <http://www.out-law.com/page-8472>

'Getting Data for Research' (ADRN, 2016) <https://adrn.ac.uk/getting-data/de-identification/>

'Investigatory Powers Bill' (GOV.UK, 7 June 2016) <https://www.gov.uk/government/collections/investigatory-powers-bill>

'Investigatory Powers Bill: May Defends Surveillance Powers' (BBC News, 15 March 2016) <http://www.bbc.co.uk/news/uk-politics-35810628>

Johnston C, 'Post Smug Vacation Statuses on Facebook, Get Your House Burgled' (*Ars Technica*, 2012) <http://arstechnica.com/tech-policy/2012/06/post-smug-vacation-statuses-on-facebook-get-your-house-burgled/>

Kelly C, 'Facebook Firing after "Friend" Boss Ripped' <http://cybersmokeblog.blogspot.co.uk/2009/08/facebook-firing-after-friend-boss.html>

'"Leaked Report" Reveals Mass Data Fears' (BBC News, 7 June 2016) <http://www.bbc.co.uk/news/technology-36469351>

'Legislative Powers: Ordinary Legislative Procedure' (European Parliament: About Parliament) <http://www.europarl.europa.eu/aboutparliament/en/20150201PVL00004/Legislative-powers>

Lomas N, 'DeepMind NHS Health Data Deal Had "no Lawful Basis"' (TechCrunch, 15 May 2017) <https://techcrunch.com/2017/05/15/deepmind-nhs-health-data-deal-had-no-lawful-basis/>

'Majority of UK MPs Back Investigatory Powers Bill in Vote' (Out-law.com: legal news and guidance from Pinsent Masons, 8 June 2016) <http://www.out-law.com/en/articles/2016/june/majority-of-uk-mps-back-investigatory-powers-bill-in-vote/>

NHS England, 'The Care.data Programme' (2016) <https://www.england.nhs.uk/ourwork/tsd/care-data/>

Nicolson S, 'What Is the Named Person Scheme?' (BBC News, 28 July 2016) <http://www.bbc.com/news/uk-scotland-scotland-politics-35752756>

Pounder C, 'Question Answered: "Why Does the European Commission Think the UK's Data Protection Act Is a Deficient Implementation of Directive 95/46/EC?". - Hawktalk' <http://amberhawk.typepad.com/amberhawk/2013/02/question-answered-why-does-the-european-commission-think-the-uks-data-protection-act-is-a-deficient-implementation-of.html>

'Reform of EU Data Protection Rules' <http://ec.europa.eu/justice/data-protection/reform/index_en.htm>

'Search in the Register' (European Council, Council of the European Union) <http://www.consilium.europa.eu/register/en/content/int/?typ=ADV&lang=EN>

Solon O, 'A Simple Guide to Care.data' (Wired.co.uk, 2014) <http://www.wired.co.uk/article/a-simple-guide-to-care-data>

——, 'The Communication of Care.data to Patients Has Been an Absolute Shambles' (Wired.co.uk, 7 February 2014) <https://web.archive.org/web/20140210042919/http://www.wired.co.uk/news/archive/2014-02/07/care-data-terrible-communication>

'The Nuremberg Code' <https://history.nih.gov/research/downloads/nuremberg.pdf>

'The Ofcom Broadcasting Code (incorporating the Cross-Promotion Code)' (Ofcom, 2016) <https://www.ofcom.org.uk/tv-radio-and-on-demand/broadcast-codes/broadcast-code>

'Thousands Descend on Tiny Dutch Town after Facebook Invitation Goes Viral' (NBC News, 22 September 2012) <http://worldnews.nbcnews.com/_news/2012/09/22/14028638-thousands-descend-on-tiny-dutch-town-after-facebook-invitation-goes-viral?lite>

Wakefield J, 'Google DeepMind's NHS Deal under Scrutiny' (BBC News, 17 March 2017) <http://www.bbc.co.uk/news/technology-39301901>

'What Happens to Your Health Data?' (The Farr Institute of Health Informatics Research) <http://www.farrinstitute.org/public-engagement-involvement/what-happens-to-your-health-data>

'What Is a Named Person?' (Scottish Government) <http://www.gov.scot/Topics/People/Young-People/gettingitright/named-person>

Appendix

Acknowledgements

To my primary supervisor, Dr Gillian Black, I owe a great deal of gratitude – not least for supervising me since my LLM and supporting me through the chaos of the last five years of a part-time PhD, consultancies, a wedding, jobs etc.! Thank you for introducing me to the wonders of data protection law & privacy, for your knowledge and expertise in these areas which contributed so greatly to my research, your constant encouragement and for keeping my eye on the prize throughout the process.

Dr Daithí MacSíthigh, for your seemingly never-ending knowledge on almost *any* area of law I ever needed help with, sticking with me even when you moved across the border (!) and your ability to keep this PhD ship calm, in even the rockiest of storms.

Professor Burkhard Schafer for your amazing insight, humour and invaluable contribution to my understanding of the public interest – maybe you are the philosopher king after all?!

I also owe a great deal of thanks to Dr Chloë Kennedy, my University of Edinburgh mentor but more aptly titled 'unofficial PhD supervisor', whose sage advice and positivity kept me sane in even the most challenging moments of the last five years!

In my adopted home in Edinburgh, I have 'boss man' (Professor Graeme Laurie!) to thank for taking a chance on me, and welcoming me into the J Kenyon Mason Institute family, which has made all the difference to my life here in Scotland. I have learned so much from working with you and I am grateful for the experience (and I hope you have learned by now that it is *always* a good idea to pack a snack bag).

I am honoured and privileged to have been awarded with the Mason Institute's first Maclagan Scholarship and hope that this thesis is a small testament to how far reaching, and enduring, Professor Mason's influence has been and will continue to be.

Being welcomed into the Mason Institute also introduced me to my 'Barbsy' (Dr Nayha Sethi!) who has gone above and beyond to support me throughout this thesis but more importantly has become a part of my family in the process. For your love, generosity, time and friendship I thank you.

To my other nearest and dearest: Kate for welcoming me so warmly to Edinburgh and continued love and positivity; Miki my 'genius friend' for your unwavering support, thoughtfulness and inspirational resilience; Carina and Kerstin for making Edinburgh feel like a friendlier place when I started this journey; and to *all* my amazing friends, colleagues and office mates who were patient and listened when I ranted, stayed silent when I would swing from doughnuts to juice cleanses, and helped me to keep my sense of humour when I had lost mine.

Without the love, support and encouragement of my Mom and Dad, from the very beginning, I simply wouldn't be here. For this I am forever grateful. (Your care packages of Reese's Peanut Butter Cups, Ghirardelli Brownies, Trader Joe's groceries galore, and anything else I just *had* to have from home, also helped. Especially with Chapter 4.)

To my brother, my Disneyland partner and constant cheerleader, thank you for keeping me laughing (often at my own expense).

To my oldest and dearest pal in the world, Nina, you have always pushed me to reach my dreams no matter how far away this would take me, and for this I know how lucky I am to have you in my life.

Finally, to my loving husband and best pal Brian. Thank you for always believing in me even when I didn't think I could do this. Without you, none of this would be possible. With you, it is worth everything. (And now, a-la-Fawlty Towers, there shall forever be *two* doctors in our household!)

Book Publisher Abbreviations

Publisher Name	Abbreviation
Oxford University Press	OUP
Cambridge University Press	CUP
Harvard University Press	HUP
Yale University Press	YUP
Princeton University Press	PUP
Stanford University Press	SUP

Table of cases

United Kingdom

Court of Justice of the European Union

European Court of Human Rights

Australia