THE HISTORY OF THE PUBLIC-PRIVATE DIVIDE IN UK INDIVIDUAL INFORMATION LAW: 1948 TO 2017

OLIVER MICHAEL BUTLER

EMMANUEL COLLEGE

AUGUST 2018

This dissertation is submitted for the degree of Doctor of Philosophy.

Preface

This dissertation is the result of my own work and includes nothing which is the outcome of work done in collaboration except as declared in the Preface and specified in the text.

It is not substantially the same as any that I have submitted, or, is being concurrently submitted for a degree or diploma or other qualification at the University of Cambridge or any other University or similar institution except as declared in the Preface and specified in the text.

I further state that no substantial part of my dissertation has already been submitted, or, is concurrently being submitted for any such degree, diploma or other qualification at the University of Cambridge or any other University or similar institution except as declared in the Preface and specified in the text.

It does not exceed the prescribed work limit for the relevant Degree Committee.

This thesis, including footnotes, does not exceed the permitted length.

CONTENTS

CHAPTER 4: THE PUBLIC-PRIVATE DIVIDE AND UK HUMAN RIGHTS

CHAPTER 5: THE PUBLIC-PRIVATE DIVIDE AND EUROPEAN DATA PROTECTION

CHAPTER 6: THE PUBLIC-PRIVATE DIVIDE AND UK DATA PROTECTION

CHAPTER 7: THE PUBLIC-PRIVATE DIVIDE AND UNAUTHORISED DISCLOSURE OFFENCES

CHAPTER 8: THE HISTORY OF THE PUBLIC-PRIVATE DIVIDE IN UK INDIVIDUAL INFORMATION LAW: COMPLEX INTERACTIONS BETWEEN DIVERSE APPROACHES

CHAPTER 1

THE PUBLIC-PRIVATE DIVIDE IN UK INDIVIDUAL INFORMATION LAW: 1948 TO 2017

INTRODUCTION

One major 21st century challenge is the regulation of information and, in particular, information about individuals. In the United Kingdom, the regulation of individual information has a history extending back to at least the 19th century. That history spans several overlapping legal regimes. In particular, those regimes are confidentiality, the right to private life, data protection, and official secrecy and unauthorised disclosure offences. The regulation of individual information is a "socio-technical problem"[1] of enormous complexity, difficulty and importance. It has emerged during a period of vast technological, social and political change and lies at the interface of technology and institutions, both public and private.

The regulation of individual information is an important aspect of the broader infrastructure within which individuals, markets and institutions act.[2] Information flows are crucial to the success of both public services and private markets, facilitated by rapid technological development. Information systems have intensified some risks of processing and using information and created newly perceived dangers for individuals and society. Intensified risk and new purported dangers in turn threaten to undermine the benefits brought about by the development of information systems and pose new challenges for regulation.

This thesis adopts an architectural perspective. It asks how and why the architecture of individual information law has been developed in relation to the public-private divide. By public-private divide, I mean the ways in which public authorities are regulated differently from private actors in relation to individual information. The overlapping legal regimes affecting individual information law have often been analysed in isolation from one another. This thesis seeks to identify common approaches to the public-private divide across the history of individual information law. The analysis demonstrates a common set of concerns and approaches across these distinct but overlapping regimes for the regulation of individual information. I use the term individual information inclusively, conscious of the differing scope of confidential, private, personal, official and official individual-identifying information or data across the areas of law studied. Although there are differences in scope, these areas all

---

[1] Helen Nissenbaum, Privacy in Context: Technology, Policy and the Integrity of Social Life (2010), p. 5.

[2] See *Ibid.* and Daniel Solove, The Digital Person: Technology and Privacy in the Information Age (2004).

regulate to a significant extent information about individuals, even if some are more comprehensive than others.

Information technologies do not operate in isolation but have social and political dimensions. Helen Nissenbaum argues that it is artificial to distinguish between technology and its application: information technologies operate as "socio-technical devices and systems".[3] She suggests it is preferable to study and evaluate socio-technical systems themselves in order to identify the risks they present.[4] Solove argues that it is helpful to think of the law regulating information in architectural terms.[5] The harms threatened by information systems and practices in institutions are "systematic and structural in nature".[6] Such an architecture can empower and disempower, protect individuals from or expose individuals to danger.[7] For Solove, privacy is both a "form of freedom built into the social structure"[8] and a "condition we create".[9]

The public-private divide, or its absence, in a crucial feature of the architecture of information law. Understanding the role that different approaches have played in the development of that divide reveals important insights about the debates at the heart of the regulation of information. This thesis identifies four approaches to the public-private divide which have been important across the development individual information law in the UK.

Four Approaches to the Public-Private Divide in Individual Information Law

This thesis develops an argument that, across the history of confidentiality, privacy, data protection, and official secrecy and unauthorised disclosure offences applicable to or in the UK, a complex set of interactions between four approaches to the public-private divide can be identified. These approaches are market, individual, state-facilitative and state-restrictive approaches. By an approach, I mean a common set of concerns, attitudes, assumptions and tendencies that purport to justify a distinctive public-private divide in individual information law. The thesis proposes the four approaches as part of an historically-grounded framework for understanding the public-private divide in individual information law. The thesis identifies trends in the importance of those approaches over time and within different branches of individual information law. It also identifies the role of diverse actors in the development of the public-private divide and their relationship to different approaches. Finally, it explains and

---

[3] Nissenbaum (2010), p. 5.
[4] *Ibid.*, p. 88.
[5] Solove (2004), p. 100.
[6] *Ibid.*, p. 97.
[7] *Ibid.*, p. 99.
[8] *Ibid.*, p. 186.
[9] Daniel Solove, Understanding Privacy (2008), p. 65.

describes the complex set of interactions between the approaches that have characterised the development of the public-private divide over the course of its development between 1948 and 2017.

Individual approaches are motivated by a central concern for the individual. Individual information affects the interests, rights and dignity of individuals in a variety of ways. Individual approaches are equally fearful of violations, risks or harms emanating from both public and private bodies. They therefore favour a high level of protection for individual information, irrespective of the nature of the body that may cause a violation, risk or harm to individuals. An individual approach results in a preference for a high and uniform level of regulation and so resists a public-private divide.

Market approaches emphasise the importance of regulation to facilitate market transactions. This is understood as both requiring the free flow of individual information and enhancing market confidence and public trust in the handling of individual information by others. Such approaches therefore favour the lowest level of regulation consistent with confidence and trust in the market. Market approaches are also generally hostile to differences in regulation between public and private bodies. This is because such differences may create barriers to the free flow of information. This results in a preference for a low and uniform level of regulation. It resists a public-private divide.

State-restrictive approaches emphasise both the special risks created by public authorities and the special obligations they owe. Such approaches therefore favour the imposition of greater restrictions and safeguards on public authorities than on private bodies. Usually, that entails greater legal restriction on the collection, use or dissemination of individual information by public authorities. Sometimes state-restrictive approaches seek to achieve their aims by imposing greater transparency requirements on public authorities to enhance accountability. These approaches therefore sometimes weaken the protection afforded to certain classes of individual information, such as information about officials, government contractors or employees. State-restrictive approaches therefore tend to support a public-private divide.

By contrast, state-facilitative approaches emphasise the special benefits of placing more information in the hands of public authorities or enhancing public authorities' ability to control individual information. These approaches emphasise the privileged role of the state in securing the public interest or the common good. They therefore favour fewer restrictions on individual information where this facilitates its use by public authorities. Sometimes, state-facilitative approaches also favour granting public authorities more robust systems to protect and control information in the performance of public tasks, in particular individual information

about officials, government contractors or employees, for example through the criminalisation of unauthorised disclosure. State-facilitative approaches therefore show a preference for a public-private divide, though one different in shape, emphasis and justification from state-restrictive approaches.

The thesis seeks to clarify the role played by these four approaches in shaping the public-private divide in individual information law across various processes and diverse institutions. The historical analysis in this thesis seeks to achieve two things. First, it demonstrates that there is a more complex interaction between the various approaches than a mere struggle between different approaches. Second, it demonstrates that there has not been a simple historical shift from one approach to the public-private divide to another, towards the erosion of the public-private divide in individual information law. In particular, there has not been a simple shift from a state-restrictive to an individual approach, even though the law has enhanced the level of protection afforded to individual information against private actors.

On the contrary, this thesis argues that these rival approaches coexist and interact. While individual approaches have indeed emerged and grown in significance, other approaches have also seen ongoing acceptance, endurance, and even resurgence. Market approaches have gained a widespread acceptance as a baseline of individual information law, though they are often transcended by other approaches. State-facilitative approaches have endured and can occasionally reassert themselves, especially where executive actors play a leading role in shaping the development a part of the law. Although the rise of individual approaches has been highly influential in eroding the public-private divide in information law, rather than falling into obsolescence, state-restrictive approaches have often resurged and played a decisive role in shaping individual information law. While there are affinities between certain approaches and institutions, which can lead to a privileging of an approach within a given institutional setting, those patterns are neither universal nor constant. The development of information law is instead dynamic and reflects complex interactions between diverse approaches. Particular institutions have adopted different approaches over the course of the history of individual information law. The thesis therefore contributes to the more normative literature on public-private divides in information law by supplying a more nuanced and historically-grounded understanding of the development of those divides in the UK and Europe.

The historically-informed theoretical framework developed in this thesis suggests that disagreement over the public-private divide does not merely reflect disagreement over the proper implementation of information rights, although that is an aspect of the divide, but also reflects core ideological disagreement about the aims and objectives of individual information law. In particular, it reflects different ideas about the nature of and threats to

individual rights, the requirements of markets, and the proper role and function of the public authorities. Rather than a lack of coherence, this points to deeper debates and themes. The public-private divide in individual information law rests on a more complex history than either a paradigmatic shift from a state-restrictive to an individual approach or mere struggle between rival approaches. A thorough understanding of this is valuable because it helps us to appreciate the diversity of approaches, concerns and agendas that have shaped individual information law. Additionally, those approaches, concerns and agendas are not unique to one branch of individual information law but are found across confidentiality, privacy, data protection, and official secrecy and unauthorised disclosure offences. A clear understanding of this diversity across individual information law is therefore important for both considering the future of the public-private divide and comprehending the existing law.

The history of the public-private divide demonstrates some instances of conflict or struggle between rival approaches but also other forms of interaction. Inconsistency across the jurisprudence can reflect diversity of thought about the public-private divide, both through compromises struck and ambiguity preserved. Multiple approaches sometimes subsist or coexist within the same body of jurisprudence or the same piece of legislation. Sometimes one approach mitigates or softens a more dominant approach within the law. Again at other points in the history of individual information law, multiple approaches favour a shared outcome: cooperation is apparent. At other points, pressure from advocates of one approach catalyse action which ultimately develops in line with a different approach. Sometimes a state-restrictive changes are introduced with a state-facilitative motive or individual rights protection is advanced with a state-facilitative concern. On other occasions, a shift in approach or emphasis can be discerned over time as minds change without an obvious break with the past: the evolution of approach over time. The type of approach adopted can shift over the course of legal development, especially as responsibility for the development of the law shifts between different institutional actors, executive, legislative or judicial, with different or evolving approaches to the public-private divide. The development of individual information law has also shifted between the European and national level, with different approaches leading to both convergence and divergence between European and national law.

In its analysis, the thesis seeks to explain the asymmetries within individual information law and the alliances, synergies, interactions, catalysts and compromises between different approaches that have shaped the public-private divide. It concludes by pointing to the wide acceptance, often transcendence, of market approaches, the endurance of state-facilitative approaches, the emergence and rise of individual approaches and the resurgence of state-restrictive approaches within individual information law. These complex interactions between

different approaches have shaped the uneven public-private divide across UK individual information law.

SCHOLARSHIP ON THE PUBLIC-PRIVATE DIVIDE IN INDIVIDUAL INFORMATION LAW

The public-private divide is a topic of serious concern in the scholarship on the regulation of information. This thesis critiques two distinctive historical narratives about the development of individual information law through a study of the public-private divide. The first narrative is that individual information law is undergoing a general, paradigmatic shift from a state-restrictive to an individual approach, resulting in the gradual erosion of a historic public-private divide. The second narrative is that individual information law is the result of struggles between state, private enterprise and the citizen. This thesis argues that neither narrative fully captures the complexity of the historical development of the public-private divide in UK individual information law.

The first distinctive narrative portrays the development of the public-private divide in individual information law as a shift from a now anachronistic state-restrictive approach towards a modern individual approach. This narrative is evident in both discussions of European human rights and European data protection.

Writing on the development of positive obligations in European human rights law, Dimitris Xenos argues that "a profound and permanent change has been brought about in the understanding and assertion of human rights",[10] whereby European human rights have "passed to its complete phase" from "an entitlement to… non-violation by state-agents" to the enjoyment of human rights against all.[11] Xenos's narrative is one of the progressive abandonment of a state-restrictive approach to human rights in favour of an expanding individual approach. This thesis suggests that a more complex set of interactions has characterised this legal development and such a profound and permanent shift cannot be found in relation to individual information law.

Peter Blume identifies the public-private divide in data protection law as a "basic issue" which causes obvious "friction" in the development of policy in European data protection.[12] He writes that in the 1960s public sector data processing was the main source of concern, with the state playing "the role of the iconic Big Brother".[13] By contrast, there is now, in Blume's view, a presumption that "the information relation between individual and

---

[10] Dimitris Xenos, The Positive Obligations of the State under the European Convention of Human Rights (2012), p. xxxi.
[11] Xenos (2012), p. 2.
[12] Peter Blume, *The Public Sector and the Forthcoming EU Data Protection Regulation* (2015) E.D.P.L. 32, 32.
[13] *Ibid.*, p. 32.

corporation should be regulated".[14] This presumption is a "basic feature of West-European data protection".[15] Blume argues that data protection is now "a primary and in some sense vanguard example of the broad application of human rights",[16] in contrast to traditional conceptions of human rights that focus the prevention of "different kinds of state abuse" of rights.[17] Lee Bygrave also notes that whereas historically many national data protection regimes in Europe "differentiated regulation" for the public and private sector, such "differentiation has largely disappeared in Europe":[18] we see an erosion of the public-private divide. This thesis highlights that a more complex interaction of approaches stands behind the legal development of data protection law. It adds historical depth and understanding to such accounts, in particular by demonstrating the role of different approaches in shaping the current law.

The second narrative addressed by this thesis is one of the development of the public-private divide as the result of struggle. Some privacy and data protection scholarship highlights the role of struggle between the state, commercial organisations and individuals. Helen Nissenbaum portrays the regulation of information as the site of intense struggles and "hard-fought interest brawls".[19] She notes the focus on "interest politics" in privacy law,[20] regretting the advantages that "corporate and government actors" enjoy,[21] which allow their priorities, interests and approaches to largely prevail over those of others.[22] Orla Lynskey has also described data protection law as involving a "tug of war for control over personal data" between "private organisations and governments" and the individual, especially over the enforcement of existing law.[23] This thesis supplements such observations of the importance of struggle with accounts of other forms of interaction between different approaches: compromise, cooperation, inspiration, catalysation, reaction, resistance, erosion, evolution, parallel coexistence and simple shifts in approach. It thereby hopes to supply a more detailed account of the ways in which different approaches have interacted to shape the public-private divide.

The theme of struggle as a key mechanism legal development is also common in the literature on Europeanisation and global governance. Daniel Wincott argues that the EU is a

---

[14] Peter Blume, *Privacy as a Theoretical and Practical Concept* (1997) 11(2) International Review of Law, Computers and Technology 193, p. 199.
[15] *Ibid*.
[16] Peter Blume, *Data Protection in the Private Sector* (2004) 47 Scandinavian Stud. L. 297, 298.
[17] *Ibid.*, p. 298.
[18] Lee Bygrave, Data Privacy Law: An International Perspective (2014), pp. 142 to 143.
[19] Nissenbaum (2010), p. 8.
[20] *Ibid.*
[21] *Ibid.*
[22] *Ibid.*
[23] Orla Lynskey, The Foundations of EU Data Protection Law (2015), p. 1.

dynamic forum "built through political contests and struggles",[24] in which it is important to avoid an assumption of coherence and rationality at the European level.[25] David Kennedy, a scholar of global governance, notes "the ubiquity of struggle"[26] in governance, of which the law is an instrument and a tool.[27] He argues that "patterns of past struggle [are] woven into the fabric of stability".[28] He further identifies a tendency of the expert participants in those struggles to "forget their struggles and their role…[in order] to celebrate their knowledge as universal, their world as ordered, their path forward aligned with progress".[29] He fears that this reduces understanding of how the present was created and how it might be changed, remarking that the "result of continuous struggle is an eerie stability it is hard to imagine challenging or changing."[30] This thesis demonstrates a much wider range of interactions beyond struggle through the history of the public-private divide, although I share Kennedy's wider conviction about the value of knowing how the present was created, in order to imagine how it might be changed.

A more complex historical account of the development of the public-private divide in information law might also contribute to normative arguments on the public-private divide in information privacy. One main concern of this scholarship is the blurring of the public-private divide through interactions between public and private bodies. For example, Solove argues that the nature of modern bureaucracy is neither wholly public nor private but is now one of mixed bureaucracy: "we are increasingly seeing collusion, partly voluntary, partly coerced, between the private sector and the government."[31] Neil Richards also argues that the public-private divide in the regulation of information is breaking down because surveillance now "transcends the public/private divide".[32] Similar points have been made by Jack Balkin, who argues that the distinction between public and private surveillance has "blurred if not vanished" because they are "thoroughly intertwined".[33] Similarly, Victoria Schwartz, writing in the context of US law, argues that the "*customary differences*" between public and private actors;[34] in terms of coercive power,[35] ability to harm "identify formation and democracy",[36]

---

[24] Claudio Radaelli, "The Europeanization of Public Policy" in Kevin Featherstone and Claudio Radaelli (eds), The Politics of Europeanization (2003), p. 30.
[25] *Ibid.*, p. 31.
[26] David Kennedy, A World of Struggle: How Power, Law, and Expertise Shape Global Political Economy (2016), p. 7.
[27] *Ibid.*, p. 11.
[28] *Ibid.*, p. 7.
[29] *Ibid.*, p. 5.
[30] *Ibid.*
[31] Solove (2004), p. 175.
[32] Neil Richards, The Dangers of Surveillance (2012-2013) 126 Harvard Law Review 1934, 1935.
[33] Jack M Balkin, The Constitution in the National Surveillance State (2008) 93 Minn. L. Rev. 1, 7.
[34] Victoria Schwartz, *Overcoming the Public-Private Divide in Privacy Analogies* (2015) 67 Hastings Law Journal 143, 149.
[35] *Ibid.*, p. 181.

access to technology,[37] and the extent of bureaucratic features;[38] are "beginning to break down in a modern world".[39] Schwartz notes that this is exacerbated by modern information sharing between the public and private sectors.[40] The historical account provided by this thesis highlights the ways in which these concerns at various points have been found in market and individual approaches and at other points challenged, or ignored, by state-restrictive and state-facilitative approaches. A nuanced historical account could enrich normative arguments about the public-private divide in individual information law.

There is also sometimes a tendency, in some normative arguments, to characterise state-restrictive concerns as anachronistic, reflecting concerns of the 1950s and 1960s, while arguing for an individual approach and characterising this approach as modern. The focus on state-restrictive and individual concerns could usefully be supplemented by more reflection on market and state-facilitative approaches and a greater consideration of the reasons for the occasional resurgence of state-restrictive approaches. For example, Simson Garfinkel argues that "the age of monolithic state control is over".[41] For Garfinkel, future technology-driven dangers lie not "in totalitarianism, but in capitalism, the free market, advanced technology, and the unbridled exchange of electronic information."[42] Although these concerns are proper ones, this thesis highlights a more complex historical picture than a straightforward shift away from the state and towards commercial actors as a source of concern. Although an individual approach has risen in importance, there is also evidence of the resurgence of state-restrictive concerns in some areas and the endurance of state-facilitative approaches and a broad acceptance of market approaches to individual information law. Privileging a narrative of paradigmatic shift carries the risk of obscuring important developments in this field.

Scholarship on the Changing Nature and Structure of the State

Several broader developments in the nature and function of the state make plausible the expectation that the public-private divide in individual information law will diminish. Given the plausibility of that hypothesis, the thesis is important in demonstrating that any assumed erosion and increased irrelevance of the public-private divide has not in fact occurred, and certainly not in a straightforward manner or on a linear trajectory. This in turn suggests that more complex processes are responsible for the public-private divide in individual

---

[36] *Ibid.*, p. 182.
[37] *Ibid.*, p. 183.
[38] *Ibid.*, p. 184.
[39] *Ibid.*, p. 149.
[40] *Ibid.*, p. 149.
[41] Simson Garfinkel, Database Nation: The Death of Privacy in the 21st Century (2000), p. 3.
[42] *Ibid.*

information law. The intertwining of public and private bodies more broadly has not undermined the continued appeal of all four approaches. The thesis therefore calls for a more careful examination of the reasons for this appeal and arguments beyond structural change. There is a need to account for the continued appeal of the different approaches.

Some scholarship sees the structure of the state as driving and determining the development of physical and legal infrastructures, which produce and process the information required by those structures. For such approaches, the structure of the public-private divide between public authorities and private actors determines the shape of the public-private divide in information law. Pierson and Leimgruber contend that welfare states presuppose, coincide with and require the "development of sufficient bureaucratic capacity" to carry out their programmes.[43] Higgs explains that it was the 20th century "rise of an all-encompassing Welfare State"[44] which led to "a vast expansion in the contacts citizens had with the central state, either as recipients of welfare, or as the payers of taxes" and "created huge flows of information and the elaboration of ever more sophisticated and anonymous systems for their storage and manipulation".[45]

The nature and function of the state in the UK has changed considerably since the 1940s. The welfare state that developed after the Second World War was restrained in the 1970s and 1980s by the growing popularity of neoliberal critiques,[46] based on a concern for efficiency and liberty, a "morally engaged conservatism" and fears that the welfare state undermined responsibility and civil society.[47] These ideological changes were accompanied by changing economic and demographic trends[48] that constrained the state's capacity, although the extent of retrenchment in the welfare state[49] and the reality of economic and demographic "crises" facing the welfare state[50] have been challenged. These economic critiques of the public services were subsequently also recognised by social democratic critiques of the welfare state. This resulted in the promotion of "quasi-markets", introducing

---

[43] Chris Pierson and Matthieu Leimgruber, "Intellectual Roots", in Francis G Castles, Stephen Leibfried, Jane Lewis, Herbert Obinger and Christopher Pierson (eds.), The Oxford Handbook of the Welfare State (2010), p. 33.
[44] Edward Higgs, The Information State in England: The Central Collection of Information on Citizens Since 1500 (2003), p. 149.
[45] *Ibid.*, p. 150.
[46] See, for example, Friedrich Hayek, The Road to Serfdom (1944) and Milton Friedman, Capitalism and Freedom (1962).
[47] Francis G Castles, Stephen Liebfried, Jane Lewis, Herbert Obinger and Christopher Pierson, "Introduction", in Francis G Castles, Stephen Leibfried, Jane Lewis, Herbert Obinger and Christopher Pierson (eds.), The Oxford Handbook of the Welfare State (2010), pp. 9 to 11.
[48] See "permanent austerity" in Paul Pierson, The New Politics of the Welfare State (2001), p. 13.
[49] *Ibid.*
[50] Francis G Castles, The Future of the Welfare State: Crisis Myths and Crisis Realities (2004).

new incentive structures for providers and choice for recipients of services.[51] Other left critiques favoured a shift to a "social investment state",[52] which would coordinate rather than deliver welfare.[53] Some commentators observe that these trends have resulted in a restructuring of welfare states, as market mechanisms became "ideationally unchallenged across the political spectrum".[54]

Majone argues that there has been a "rise of the regulatory state to replace the dirigiste state of the past":[55] a shift from the "positive to the regulatory state".[56] The regulatory state adopts the role of "umpire" over privatised services rather than being the "producer of goods and services".[57] It relies on regulation rather than "public ownership, planning or centralised administration".[58] This more limited state role reflects "budgetary limitations on the activities of regulators", who are able to externalise the costs of compliance.[59] Due to this, the "state steers [but] it does not row".[60] Different information systems are required to carry out the tasks of the regulatory state.

Gilbert points to a paradigm shift from "welfare state" to "enabling state", although Gilbert denies that it exists anywhere in a "pure form".[61] Gilbert advances a convergence thesis in respect of the enabling state: within certain parameters the shift is an *inevitable one*.[62] The shift from welfare state to enabling state entails a shift from a "universal approach" to a "selective approach" to benefits and from "public delivery" to "private delivery".[63] Gilbert identifies the "privatisation of social welfare" and an "increased targeting of benefits" as two key trends associated with this shift.[64]

---

[51] See Julian Le Grand, Motivation, Agency and Public Policy: Of Knights and Knaves, Pawns and Queens (2003).
[52] Anthony Giddens, The Third Way: The Renewal of Social Democracy (1998).
[53] Desmond King and Fiona Ross, "Critics and Beyond", in Francis G Castles, Stephen Leibfried, Jane Lewis, Herbert Obinger and Christopher Pierson (eds.), The Oxford Handbook of the Welfare State (2010), p. 54.
[54] *Ibid.*, pp. 55 to 56; see also Paul Pierson, Dismantling the Welfare State? Regan, Thatcher and the Politics of Retrenchment (1994).
[55] Giandomenico Majone, *The Rise of the Regulatory State in Europe* (1994) 17(3) West European Politics 77, 77.
[56] Giandomenico Majone, *From the Positive to the Regulatory State: Causes and Consequences of Change in the Mode of Governance* (1997) 17(2) Journal of Public Policy 139, 139.
[57] Majone (1994), p. 80.
[58] *Ibid.*, p. 77.
[59] *Ibid.*, p. 87.
[60] David Osbourne and Ted Gaebler, Reinventing Government: How the Entrepreneurial Spirit is Transforming the Public Sector (1992).
[61] Neil Gilbert, Transformation of the Welfare State: The Silent Surrender of Public Responsibility (2002), pp. 4 and 46 respectively.
[62] *Ibid.*, p. 42.
[63] *Ibid.*, p. 3.
[64] *Ibid.*, p. 5.

Vincent-Jones argues that a "radical transformation" is occurring as the UK replaces "bureaucratic monopolies" with "competitive quasi-markets", through a process "whereby public service functions are performed increasingly by private firms or semi-autonomous state or voluntary bodies in contractual relationships with public purchasing agencies".[65] This involves indirect and regulatory controls over direct and bureaucratic controls.[66] It also entails the use of "contract by public purchasers as a regulatory mechanism".[67] As a result of this, there is both "governance of contract" and "governance by contract",[68] each of which will produce a need for information that is not found in systems of bureaucratic control.

For Moran, there has been a change of "epoch", as yet incomplete,[69] driven by the fall of Keynesianism.[70] This entails a shift from "tacit knowledge" to "the expansion of audit into ambitious systems of surveillance".[71] This requires for more expansive information gathering and use.

Other approaches to the regulatory state have also reflected the changing relationship between public and private actors. For example, risk-based approaches rely on fewer resources and more prioritisation and targeting. Black claims that "risk is fast becoming the central organising principle in regulation and public service delivery" to target resources.[72] Such measuring and monitoring risk requires extensive information systems.

Public and private actors tasks are increasingly intertwined and supported by information flows. Scott writes that regulatory resources, including information, are "dispersed and fragmented" both "among state bodies, and between state and non-state bodies".[73] He notes that the dissemination of information can undermine the informal authority of the "information rich" by redistributing the balance of information resources.[74] The result is a transformation in the way the state interacts with the market. Pierson and Leimgruber suggest that the regulation of information will develop to support targeting and will facilitate information flows between public authorities and private contractors.[75] Commentators in the US note this

---

[65] Peter Vincent-Jones, *The Regulation of Contractualisation in Quasi-Markets for Public Services* (1999) Public Law 304, 304.
[66] *Ibid.*, p. 310.
[67] *Ibid.*, p. 313.
[68] *Ibid.*, p. 316.
[69] Michael Moran, The British Regulatory State: High Modernism and Hyper-Innovation (2003), p. 179.
[70] *Ibid.*, pp. 2 to 7.
[71] *Ibid.*, p. 7.
[72] Julia Black, *The Emergence of Risk-Based Regulation and the New Public Risk Management in the United Kingdom* (2005) Public Law 512, 512.
[73] Colin Scott, *Analysing Regulatory Space: Fragmented Resources and Institutional Design* (2001) Public Law 329, 330.
[74] *Ibid.*, p. 347.
[75] Pierson and Leimgruber, "Intellectual Roots" in Castles, Leibfried, Lewis, Obinger and Pierson (eds.) (2010), p. 33.

"peculiar vulnerability of the needy and dependent to official or quasi-official inquiry and surveillance"[76] due to the "pervasive requirement of establishing need"[77] through the "means test"[78] and in order to combat fraud.[79] The need to target resources and interventions lead public authorities to "concentrate on the unique personal circumstances of the recipients" which "require intimate knowledge" of the individual's circumstances.[80]

Although certainly important phenomena, the thesis resists the conclusion that the development of individual information law follows the structure and function of the state and its interaction with private actors. Undoubtedly, these trends are important for understanding the attractions and justifications for different approaches. This thesis resists the inference of inevitability in favour of a more nuanced understanding of the influence of different approaches to the public-private divide. The thesis hopes to provoke a deeper consideration of the reasons for the persistence of other approaches and their values.

Emphasis on Revolutionary Change in the Information Society: Continuities in the Public-Private Divide

The broader literature on the information society also places an emphasis on revolutionary change driven by information technology. This thesis challenges those broader deterministic and revolutionary expectations by demonstrating the recurrence of four approaches to the public-private divide. This recurrence is a point of continuity despite technological change. Despite the revolutionary nature of change claimed more broadly, a distinctive set of approaches to the public-private divide have shaped information law since the 1940s. The thesis should therefore give pause for thought about radical claims of change driven by information technology.

The variety of complex interactions between different approaches identified in this thesis contradict deterministic claims made in the literature on the information society. Scholarship on the information society commonly emphasise narratives of change as a frame for legal development. Changes in technology and its use will disrupt existing regimes and produce a very different regulatory landscape. These changes sometimes describe the shift to an information society as a third revolution, after the agrarian and industrial revolutions: an information revolution.[81]

---

[76] Joe Handler and Magaret Rosenheim, Privacy in Welfare: Public Assistance and Juvenile Justice (1966) Law and Contemporary Problems 377, 377.
[77] *Ibid.*
[78] *Ibid.*, p. 380.
[79] *Ibid.*, p. 383.
[80] *Ibid.*, p. 379.
[81] Alvin Toffler, The Third Wave (1980).

There is a tendency to suggest that revolutionary developments will inevitably result in revolutionary approaches to law, institutions and information. This thesis does not dispute that important and far-reaching changes are occurring. Neither does it doubt that such change presents new challenges for the regulation of information. Nor does it challenge the view that information and technology are changing the way that individuals, institutions and law interact. This thesis instead seeks to argue that, within these narratives of change, there subsists an important point of continuity. That point of continuity takes the shape of an enduring and complex interaction between different approaches to the public-private divide at the heart of historical debates and attempts to regulate information.

The literature on technological development and the information society contains deterministic claims about the historical impact of technology. Although this determinism is not directed at the public-private divide, the historically-grounded theoretical framework identified points against the deterministic historical claims of the broader literature. Technological determinism is a theme of discussions on the impact of rapid changes in information technology. The changes brought about by information technology are often understood as revolutionary[82] or inevitable in nature.[83] Stubbs characterises the modern period as a "post-information age period of sustained disruption and change",[84] in which he compares modern technology-driven change to the industrial revolution and its significant impact on the nature of society".[85] Toffler compares the changes in information technology to the industrial revolution, entailing a "radical shift of direction" in society.[86] Gates argues that the "global interactive network will transform our culture as dramatically as Gutenberg's press did the middle ages".[87] Castells makes a similar comparison, arguing that it will introduce "a pattern of discontinuity in the material basis of economy, society and culture".[88] Negroponte makes the strong deterministic claim that "like a force of nature, the digital age cannot be stopped".[89] Coyle sees the changes brought about by technology as "inexorable".[90]

Some have resisted deterministic rhetoric in the literature on the information society. May resists the view that the information society marks "the dawning of a new age" in which old

---

[82] Christopher May, The Information Society: A Sceptical View (2002), p. 21.
[83] *Ibid.*, pp. 21 and 23.
[84] Evan Stubbs, Big Data, Big Innovation: Enabling Competitive Differentiation Through Business Analytics (2014), p. 14.
[85] *Ibid.*, p. 21.
[86] Toffler (1980), p. 366.
[87] Bill Gates, The Road Ahead (1996), p. 9.
[88] Manuel Castells, The Rise of the Network Society (1996), p. 3.
[89] Nicholas Negroponte, Being Digital (1995), p. 229.
[90] Diane Coyle, Economics: The Weightless Economy (1997), p. 23.

understandings are "immediately invalidated".[91] It is not, in May's view, the "end of history".[92] He criticises "tales of transformation" as exaggerations.[93] May considers that the "vision of an information society itself often takes the character of an all-encompassing story about this new age".[94] He is sceptical about the profundity, though not the fact, of change, instead emphasising continuities.[95]

May comments that "this disjuncture with the past" is one which "resonates throughout the literature of the information society",[96] where there is a "common perception of inevitability" about the changes wrought by technology.[97] May criticises the "unidirectional determinism" assumed by "overarching claims for revolution".[98] Hamelink similarly criticises the information society as a "powerful myth" that "the 'information revolution' is the most significant historical development of our time".[99] For May, these characterisations of the information society are ultimately historical claims.[100] May emphasises "human agency in the history of technology"[101] and argues:

> There is nothing natural, nothing inevitable about the information society: while we can only make our own history in the circumstances we find ourselves in, we should recognize that these circumstances are not as fixed or narrow as many commentators on the information society tell us.[102]

May's rhetoric is perhaps too strong. The strong claim of choice is an overreaction to deterministic narratives. This thesis indicates broad erosions of the public-private divide in response to change. However, it also highlights its nuances and the role of other approaches. Although there is not inevitability, neither can we fully discount the influence of broad societal and technological trends. The thesis instead points to a more complex and nuanced history, the role of diverse actors and approaches and therefore resists historical determinism.

---

[91] May (2002), preface, pp. viii and ix.
[92] *Ibid.*
[93] *Ibid.*, p. 1.
[94] *Ibid.*
[95] *Ibid.*, p 2.
[96] *Ibid.*, p 8.
[97] *Ibid.*, p 13.
[98] *Ibid.*, pp. 13 to 14.
[99] Cees Hamelink, "Is there Life after the Information Revolution?", in Michael Trabner (ed.), The Myth of the Information Revolution: Social and Ethical Implications of Communication Technology (1986), p. 7.
[100] May (2002), p. 19.
[101] *Ibid.*, p. 29.
[102] *Ibid.*, p. 161.

ADOPTION OF A HISTORICAL APPROACH TO THE PUBLIC-PRIVATE DIVIDE

This thesis is a response to calls for more historical analysis regarding the regulation of information.[103] Individual information law in the UK stands at a significant watershed in its history. It is on the brink of an important and as yet unclear process of change regarding the UK's position in respect to the rest of Europe. A study of the history of individual information law during the period in which it grew dramatically and closely with Europe is of value in understanding the current law and thinking about its future.

In particular, the thesis argues that a state-restrictive approach is not just an artefact of thought before the 1960s but has a continuing appeal and vibrancy. It cannot be disregarded as an approach in the future. The endurance of state-facilitative approaches show that this approach similarly cannot be disregarded in the future. The widespread acceptance of market approaches, even if often transcended, speaks to a floor of individual information law that similarly cannot be disregarded. Finally, even if perhaps threatened by Brexit, the individual approach that owed much to Europeanisation in privacy and data protection law has firmly risen and so cannot be disregarded. The thesis hopes to enrich our understanding of the origins of the public-private divide in UK individual information law and, in identifying the complexity of its development and resistance to erosion, identify those approaches that will continue to influence its future development: ideas about individual rights and interests in information and rival conceptions of the role of the state and the needs of markets.

A historical approach is best able to demonstrate the complex interaction of the four approaches throughout the period examined: 1948 to 2017. This period was chosen to examine the modern law throughout a distinctive period of Europeanisation. As the UK took decisive steps to alter its relationship with Europe in March 2017 by notifying the EU of its intention to withdraw, this thesis focuses on legal developments up to 2017.

There are important early signs that the development of individual information law shifted its focus to a post-Brexit future following this date. Although the Data Protection Act 2018, which received royal assent on 23 May 2018, implements the EU Law Enforcement Directive and supplements the GDPR, it was an Act passed in the shadow of Brexit. National policy during the passage of that legislation focused on the position of the UK's data protection laws post-Brexit. For example, on 7th August 2017 Matt Hancock MP, then Minister of State for Digital, highlighted that bringing EU law into domestic law with the then Data Protection

[103] See Lee Bygrave, "Legal Scholarship on Data Protection: Future Challenges and Directions", in Terwangne, Degrave, Dusollier and Quick (eds.), Liber Amicorum Yves Pollet: Essays in Honour of Yves Pollet (2018); Higgs (2003), p.11.

Bill "will ensure that we help to prepare the UK for the future after we have left the EU".[104] The Department for Digital, Culture, Media, and Sport also emphasised the importance of the Bill for maintaining "uninterrupted" data flows post-Brexit.[105] The UK Government's August 2017 position paper, The Exchange and Protection of Personal Data: A Future Partnership Paper, in turn advocated a "UK-EU model for exchanging and protecting personal data, which could build on the existing adequacy model" for third countries.[106] There are similarly clear indications that European policy shifted to a focus on the UK post-Brexit by the end of 2017. For example, on 9th January 2018, the European Commission confirmed in a "Notice to Stakeholders" that the General Data Protection Regulation (GDPR) would cease to apply to the UK as a matter of EU law, in the absence of ratified withdrawal agreement, on 30 March 2019.[107] Negotiations had advanced considerably on post-Brexit data protection, as evidenced by Article 66 and 67 of the Draft Withdrawal Agreement, by March 2018,[108] although there remains a lack of agreement on the final draft at the time of writing. Given the uncertainty around the final outcome of these negotiations and the shift in focus apparent in national and EU policy by the end of 2017, this thesis takes 2017 as the end of a distinctive period of legal development. The Data Protection Act 2018 is addressed briefly where relevant to the implementation of the GDPR only.

Glyn Watkin has observed that awareness of a "European dimension to English legal developments" is a "recurring theme among contemporary historians of English law".[109] This thesis is no exception, drawing on the Europeanisation literature to help understand processes of legal change in information law in the UK. Higgs describes the developing relationship between the state, information and citizens in the UK as a "long, complex and discontinuous process".[110] He argues that it requires a "more complex, and interesting, history of information".[111] Bygrave, reflecting on the future of data protection scholarship, also highlights additional reasons to be attentive to the history of this field.[112] He argues that historical analysis can provide an opportunity to reflect upon the "rich heritage" of data

---

[104] Department for Digital, Culture, Media and Sport, A New Data Protection Bill: Our Planned Reforms, Statement of Intent, 7 August 2017, pp. 2 to 3.
[105] *Ibid.*, p. 24.
[106] HM Government, The Exchange and Protection of Personal Data: A Future Partnership Paper, August 2017, p. 2.
[107] European Commission, Notice to Stakeholders, Withdrawal of the United Kingdom from the Union and EU Rules in the Field of Data Protection (9th January 2018).
[108] Draft Agreement on the Withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and European Atomic Energy Community TF50 (2018) 35 (19 March 2018), Articles 66 and 67.
[109] Thomas Glyn Watkin, *The Future of Legal History* (2000) 7 International Journal of Legal Profession 125, 127.
[110] Higgs (2003), p. viii.
[111] *Ibid.*, p. 11.
[112] Bygrave (2018).

protection law as it develops.[113] Historical analysis is able to supplement the broader scholarship in ways that resist both "pressures to specialise" and "a fracturing of data protection scholarship into silos of discourse that rarely speak with, let alone acknowledge, one another".[114] This thesis seeks to contribute to the historical literature on information law in response to all these concerns by drawing identifying common approaches and complex historical interactions across a broad range of fields within information law.

More generally, Allison argues that legal history can improve the quality of deliberation surrounding legal development, change and reform.[115] It can help us to avoid accounts which succumb to a simplistic "Whig history" with a disguised normative agenda, it can free current thinking from historical accident, and can demonstrate the continuing importance of historical choices bound up with current arrangements.[116]

This thesis is legal historical in method. It uses detailed analysis of legislation, case law, parliamentary debates, preparatory and policy materials to identify the approaches taken by executive, legislative, judicial and regulatory actors both in the UK and Europe, where European law has either been implemented in the UK or has otherwise influenced the adoption of legislation. It takes as its period 1948 to 2017, from drafting the treaties that became the ECHR and EU and arguably the first modern confidentiality case law in the UK[117] to the start of negotiations for Brexit, which place in doubt the continuing shape of data protection in the UK and mark a new, and perhaps a quite different, phase of Europeanisation.

The period 1948 to 2017 represents a distinctive period of Europeanisation in UK information law and this thesis draws on the literature on Europeanisation processes to inform its historical approach. It takes this broad approach to a narrow concept to illustrate the wide application of the four-model framework to the development of information law, underlining its usefulness for understanding information law debates. This is important because it highlights the importance of engagement with the theories and arguments that underpin those struggles and debates as the UK negotiates a new relationship with European institutions and evaluates the case for change in a global landscape.

---

[113] *Ibid.*, p. 8.
[114] *Ibid.*, pp. 3 to 4.
[115] John Allison, *History to Understand, and History to Reform, English Public Law* (2013) Cambridge Law Journal 526.
[116] John Allison, *History in the Law of the Constitution* (2007) 28 Journal of Legal History 263.
[117] *Saltman Engineering Co v Campbell Engineering Co* (1948) 65 RPC 203.

A HISTORICAL APPROACH INFORMED BY SCHOLARSHIP ON EUROPEANISATION

The historical approach in this thesis is informed by the broader scholarship on Europeanisation. That scholarship also addresses the limits of models of history as either struggle or as a linear paradigmatic shift. The scholarship instead highlights the complexity of interactions between ideas and institutions in the process of Europeanisation. Although it acknowledges the role of struggle, it goes beyond it. Finally, it acknowledges the ways in which legal development can shift between European and national levels.

This thesis is intended to engage with an aspect of the "ontological challenge" within the literature on Europeanisation. The challenge seeks to identify the role of agency and structure in the development of European law. The history of UK individual information law 1948 to 2017 is a European history. It is deeply connected with the development of individual information law from the European Convention on Human Rights (ECHR), the Council of Europe, and in the European Union (EU). The thesis demonstrates how a four-approach framework can enrich a historical understanding of the complex, inconsistent and diverse legal architecture that has developed in relation to the public-private divide in UK individual information law. In doing this, it better reveals the agency of those engaged in the development of the law regulating information and the choices that prevailed in debates between executive, legislative, judicial and regulatory elites, as well as the structural features that sometimes privilege particular approaches.

The thesis addresses the ontological challenge of understanding Europeanisation by drawing attention to the role of various elites in the development of the law and explaining the approaches that motivate, frame or resolve their conflicts. Featherstone defines the "ontological challenge" of Europeanisation as a challenge "to clarify the role of structure and agency within the Europeanization process, whilst identifying the mechanisms that are the interactive link between the 'domestic' and the 'EU' spheres of activity."[118] He observes that the relationship between "cause and effect" is "deceptive"[119] and the "the relationship between structure and agency is by no means simple."[120] Europeanisation was by no means uniform across the law of confidentiality, the right to private life, data protection and the criminalisation of unauthorised disclosures. This thesis helps to highlight that uneven European influence across individual information law.

The Europeanisation literature is sceptical of deterministic theories of change. In this it can be contrasted with aspects of the literature on technology and information society which

---

[118] Kevin Featherstone, "Introduction: In the Name of 'Europe'", in Kevin Featherstone and Claudio M Radaelli, The Politics of Europeanization (2003), p. 13.
[119] *Ibid.*, p. 4.
[120] *Ibid.*

emphasise the inevitability of certain changes in information technology law, a form of technological determinism, and literature on the changing structure and function of the state which emphasises the inevitability of changes in the bureaucratic capacity of the state in relation to information, a form of structural determinism. In identifying a point of continuity rooted in a conceptual tension which forms the subject matter of complex interactions, this thesis speaks to themes of ongoing agency and choice in the face of these various deterministic claims and integrates the history of the public-private divides in UK information law into the literature on Europeanisation by showing the extent to which legal development is non-linear, fragmented, and shaped by agency and choice.

The concept of Europeanisation is subject to a wide variety of definitions.[121] It has enjoyed popularity as a "fashionable term" in politics and international relations[122] and has been the subject of research for over 30 years.[123] The literature has an important historic focus.

Europeanisation itself can be viewed as a historical process.[124] Featherstone and Radaelli consider that "Europeanisation is not so much a theory as a distinct set of processes in need of explanation."[125] Although reference to "domestic adaptation to the pressures emanating directly or indirectly from EU membership" is the most common scope of the term,[126] other definitions are broader in scope, treating Europe as a region or including European institutions such as the Council of Europe or the ECHR.[127] This thesis adopts a broader definition of Europe to include such institutions. It does this because it takes an inclusive approach to the definition of individual information law.

Europeanisation must be distinguished from several related or similar concepts. It is not neo-functionalism. Neo-functionalism is narrower than Europeanisation and relates to a change whereby actors prefer European integration.[128] Europeanisation by contrast covers a broader range of changes in response to Europe. It is not integration, which is an institutional process of pooling national sovereignty.[129] Europeanisation concerns the effects resulting, in part, from that integration.[130] It is not merely EU policy formation.[131] Rather, Europeanisation

---

[121] *Ibid.*, p. 5.
[122] *Ibid.*, p. 3.
[123] Kevin Featherstone and Claudio Radaelli, "A Conversant Research Agenda", in Featherstone and Radaelli (eds.) (2003), p. 331.
[124] Featherstone, "Introduction: In the Name of 'Europe'", in Featherstone and Radaelli (2003), p. 5.
[125] Featherstone and Radaelli, "A Conversant Research Agenda", in Featherstone and Radaelli (eds.) (2003), p. 333.
[126] Featherstone, "Introduction: In the Name of 'Europe'", in Featherstone and Radaelli (2003), p. 7.
[127] Claudio Radaelli, "The Europeanization of Public Policy", in Featherstone and Radaelli (eds.) (2003), p. 31.
[128] Featherstone, "Introduction: In the Name of 'Europe'", in Featherstone and Radaelli (2003), p. 8.
[129] Radaelli, "The Europeanization of Public Policy", in Featherstone and Radaelli (eds.) (2003), p. 33.
[130] *Ibid.*, p. 33.
[131] *Ibid.*, p. 34.

concerns “the penetration of the European dimension in national arenas of politics and policy”.[132] EU policy formation does not concern implementation at the national level. Europeanisation is also not simply harmonisation or convergence.[133] As Radaelli notes, these are consequences, and not necessary consequences, of Europeanisation, which may also result in divergence.[134]

The scholarship on Europeanisation provides two different accounts of the effect of Europeanisation on national legal development.[135] Borzel characterises these as structuralist vs agency-centred accounts.[136] Structuralist accounts argue that Europeanisation should cause “structural convergence”.[137] Jaaskinen argues that national legal systems tend to “limit Europeanisation that threatens their own coherence” but convergence is ultimately inevitable due to Europeanisation itself.[138] Agency-centred accounts anticipate a greater degree of divergence at the national level and the uneven implementation of European norms.[139] This is due to the role played by “change agents” such as norm entrepreneurs and epistemic communities.[140] This thesis traces a middle way, conscious of the role played by both structure and agency but resistant to determinism. Instead it understands the agency of various actors as shaped by different approaches to the public-private divide.

The thesis also draws on rational institutionalism in acknowledging the role of structure on legal development.[141] Rationalist institutionalism posits that “the absence of multiple veto points and the presence of supporting institutions” encourage change.[142] Equally, the existence of veto points and unsupportive institutions create opportunities for divergence or resistance. These structural features do not explain why actors choose change but it does sometimes help to explain why they succeed or fail in realising their preferences. Accordingly, the thesis observes that the complex interactions between the four approaches identified shape the agency of actors while structural factors sometimes help to explain the nature and result of those interactions.

---

[132] *Ibid.*, p. 29.
[133] *Ibid.*, p. 33.
[134] *Ibid.*
[135] Tanja Borzel, “Conceptualizing the Domestic Impact of Europe”, in Kevin Featherstone and Claudio Radaelli (eds.), The Politics of Europeanization (2003), p. 66.
[136] *Ibid.*, p. 66.
[137] *Ibid.*
[138] Niilo Jaaskinen, *Europeanisation of National Law: A Legal-Theoretical Analysis* (2015) European Law Review 667, 681.
[139] Borzel, “Conceptualizing the Domestic Impact of Europe”, in Featherstone and Radaelli (eds.) (2003), p. 66.
[140] *Ibid.*, p. 67.
[141] *Ibid.*, p. 74.
[142] *Ibid.*

As Borzel observes, rationalist or sociological institutionalist accounts can operate "simultaneously or characterize different phases in processes of adaptational change".[143] This thesis illustrates this in relation to information law. Featherstone and Radaelli explain that "Europeanisation is not producing a coherent, homogeneous, and harmonized Europe" because there is a great deal of diversity between states in terms of the "role of the state in the economy, the scope of the welfare state, the functions of social policy".[144] Europeanisation "has a differential or asymmetrical impact".[145] Europe is a "complex reality" with elements of both convergence and fragmentation.[146] Featherstone emphasises that the "impact of Europeanisation is typically incremental, irregular, and uneven over time and between locations, national and subnational."[147] Europeanisation as a research agenda is an examination of asymmetries.[148] Those asymmetries are asymmetries of "absorption, accommodation, and transformation".[149] For Featherstone, Europeanisation as a field of research "acknowledges the dynamism, imbroglio, and limits to determinism in present-day Europe."[150] Goetz argues that the EU should be understood as "arena" rather than "actor", with processes that are "circular rather than unidirectional, and cyclical rather than one-off".[151] Such observations are reflected in this thesis.

STRUCTURE OF THE THESIS

The thesis critiques the two narratives that individual information law consists of a gradual erosion of the public-private divide in light of an increasingly individual approach and that individual information law was produced by struggle, across four major areas of individual information law: confidentiality, the right to respect for private life, data protection and the criminalisation of unauthorised disclosures, including official secrecy. In doing this, it demonstrates that the rise of an individual approach has also often been accompanied or followed by the resurgence of a state-restrictive one. State-facilitative approaches have also endured and reoccurred at various points in the history of individual information law. The

---

[143] *Ibid.*
[144] Featherstone and Radaelli, "A Conversant Research Agenda", in Featherstone and Radaelli (eds.) (2003), p. 336.
[145] *Ibid.*, p. 338.
[146] *Ibid.*, p. 340.
[147] Featherstone, "Introduction: In the Name of 'Europe'", in Featherstone and Radaelli (eds.) (2003), p. 4.
[148] *Ibid.*, p. 18.
[149] *Ibid.*, p. 19; Borzel, "Conceptualizing the Domestic Impact of Europe", in Featherstone and Radaelli (eds.) (2003), pp. 69 to 70.
[150] Featherstone, "Introduction: In the Name of 'Europe'", in Featherstone and Radaelli (eds.) (2003), p. 19.
[151] Radaelli, "The Europeanization of Public Policy", in Featherstone and Radaelli (eds.) (2003), p. 34; Klaus Goetz, *Four Worlds of Europeanisation*, paper prepared for the ECPR Joint Sessions of Workshops, Turin, Italy, 22 (7th March 2002) p. 4.

acceptance of market approaches have also frequently played an important role in the erosion of the public-private divide. In addition to struggle, these areas of law demonstrate a broader set of complex interactions between the four approaches identified, including tensions, compromises, catalysts, reactions, parallel coexistence and shifts between the approaches over time.

In chapter 2, I examine the development of legal doctrines regulating confidential information. In chapter 3, I examine the development of European human rights law on the right to respect for private life, in so far as it touches upon individual information. In chapter 4, I consider the implementation of that European human rights law in the UK. In chapter 5, I analyse the development of European data protection law and, in chapter 6, its implementation in the UK. Finally, in chapter 7, I examine the development of the criminalisation of unauthorised disclosures, through the history of official secrecy and the plethora of individual-identifying unauthorised disclosure offences that multiplied after reform of official secrecy in 1989. In chapter 8, I conclude that an understanding of the complex interactions between the four approaches identified provides a more accurate historically-grounded theoretical framework for explaining the development of the public-private divide in UK individual information law than other common narratives of legal change in this field.

CHAPTER 2

THE PUBLIC-PRIVATE DIVIDE AND CONFIDENTIALITY

INTRODUCTION

Confidentiality has a long history as a branch of information law. It has played an important role in protecting individual information, although it also protects a much wider range of information than purely individual information. It was especially important in this regard before the development of the right to private life and data protection. The thesis therefore examines the public-private divide in relation to confidentiality first.

The history of legal doctrines concerning confidentiality illustrates the role of all four approaches to the public-private divide in its development. Save for the development of the tort of misuse of private information from breach of confidence after the Human Rights Act 1998,[1] this was a national judicial project, in which the law developed with little direct European influence. First, a market approach has always informed the law on confidentiality. This approach was highly influential in its early development, though it was later transcended by other approaches. It remains a baseline in the law of confidentiality. Second, an individual approach exercised consistent influence to protect individuals' confidential information in a widening range of circumstances, which went beyond the market. Confidential information itself, protected against any party and not merely where a confidential relationship existed, was arguably protected against all by 1990. This was to be substantially strengthened in relation to private information, which substantially overlaps with confidential information, after the introduction of the Human Rights Act 1998.[2] The two approaches, market and individual, have therefore coexisted in parallel within the jurisprudence with the individual approach gradually expanding over time.

However, to understand the development of the law of confidence as a gradual shift from a market to a more individual approach under the influence of growing concern for individual privacy would ignore important counter trends in the law regulating confidentiality and public authorities. Both state-restrictive and state-facilitative approaches have shaped distinct parts of the law of confidentiality. Important state-facilitative trends include generous public interest defences for disclosure to public authorities from the late 1960s to at least the 1990s and other state-facilitative duties of confidence to the Crown. State-restrictive duties of confidence, albeit alongside state-facilitative exceptions, developed in the 1990s in relation

[1] This is addressed in chapter 4 on the implementation of the right to private life in national human rights law.
[2] *Attorney General v Guardian Newspapers Ltd (No 2)* [1990] 1 AC 109. Not all private information is necessarily confidential information, not all confidential information private information.

to information obtained in the exercise of official power. Analysis of these doctrines demonstrates a tension between state-facilitative and state-restrictive approaches. That tension operated in addition to market concerns. These developments ran parallel to the adoption of a more individual approach in relation to information that was confidential independently of a relationship of confidence or information that was private information about individuals for the purpose of the tort of misuse of private information. Further, the state-restrictive approach has had a resurgence in more recent case law on the scope of statutory exemptions to duties of confidence owed by public authorities.[3]

This analysis resists conclusions that the public-private divide is developing along a simple trajectory towards the obsolescence of the public-private divide. It also demonstrates the importance of complex interactions between the four approaches over the history of the law of confidence.

THE PROTECTION OF CONFIDENCE

The protection of confidentiality, in UK common law and equity, has a long history stretching back beyond 1948. It represents some of the earliest information law in the UK. The modern action for breach of confidence is, however, usually dated to the 1948 decision in *Saltman Engineering Co v Campbell Engineering Co*.[4] As Glover notes, the underlying policy of the law of confidentiality has not been consistent at all times and in all respects.[5] These different policies reflect differences in approach to the public-private divide in information law.

Confidentiality has long been influenced by the concerns of the market approach.[6] Glover observes that "confidence of the business or industrial sort… can be rationalised under economic and moral headings",[7] which rely on the law of confidentiality to enhance productivity and maintain "business ethics and good faith in commercial dealings".[8] In 1980, Wacks similarly observed that traditional breach of confidence was more concerned to "protect the business interests of the plaintiff rather than his interests in preserving privacy".[9] In 1998, Barber wrote that "breach of confidence primarily operates in the commercial sphere, protecting companies from errant employees capitalising on sensitive information".[10]

---

[3] *R (Ingenious Media) v Commissioners for Revenue and Customs* [2016] UKSC 54; [2016] 1 WLR 154.
[4] (1948) 65 RPC 203.
[5] John Glover, *Is Breach of Confidence a Fiduciary Wrong? Preserving the Reach of Judge-Made Law* (2001) Legal Studies 594, 599.
[6] See below, pp. 28 to 31.
[7] *Ibid.*, p. 599.
[8] *Ibid.*, p. 600.
[9] Raymond Wacks, The Protection of Privacy (1980), p. 16.
[10] Nicholas Barber, *Privacy and the Police: Private Right, Public Right or Human Right?* [1998] Public Law 19, pp. 19 to 20.

However, even before the Human Rights Act 1998 had any impact on the development of the law of confidentiality, an individual approach had also started to inform the development of the law.[11] Aplin noted that "privacy interests" had been protected by the law of confidence "albeit in a partial fashion" before the passage of the Human Rights Act 1998.[12] However, neither did the law of confidentiality lack a public-private divide.[13] As Barber stated in 1998 in relation to confidentiality:

> It is commonly supposed that English law does not possess a *droit administratif* analogous to that found in French law; there are no special rules governing private law rights in tort and contract. This is a bold statement that is more venerated than followed.[14]

The law on confidentiality has addressed a range of relationships: commercial, private and governmental.[15] The law played a role in protecting "the boundaries" of those relationships.[16] The law itself was shaped by the particular context, including whether the duty involved a public authority or private actor.[17]

This chapter analyses the development of confidentiality at common law and in equity and identifies three trends relevant to the public-private divide. In all of this, the UK courts have shown themselves to develop the common law and equity flexibly, demonstrating a key role for the national courts in developing the public-private divide in UK individual information law.

First, at its core, breach of confidence was about the protection of commercially valuable information and business relationships. A market approach underpinned the public-private divide in this respect, with confidential information protected against both public and private actors engaged in commercial transactions. The early law of confidentiality developed from private litigation between private parties and reflected limited regulation of information to promote the functioning of the market.[18] This approach, though sometimes overtaken by other approaches, has remained a consistent feature of the law of confidentiality. It protects individual information in the service of the needs of the market.

Second, breach of confidence has expanded to recognise an increasing number of private relationships as carrying duties of confidence. This ever-widening set of relationships more

---

[11] See below, pp. 31 to 33.
[12] Tanya Aplin, *The Development of the Action for Breach of Confidence in a Post-HRA Era* (2007) Intellectual Property Quarterly 19, 19.
[13] See below, pp. 33 to 51.
[14] Barber [1998], p. 21.
[15] Shelly Wright, *Confidentiality and the Public/Private Dichotomy* (1993) European Intellectual Property Review 237, 237.
[16] See *Ibid.*, pp. 238 to 239.
[17] See *Ibid*.
[18] See below, pp. 28 to 31.

clearly reflects the development of breach of confidence as a protection for the private lives of individuals. Confidentiality therefore increasingly reflected an individual approach beyond a market approach. This arguably extended so far as information which was confidential itself, without a particular relationships, and later to all private information.[19] Of course, one of the most important developments in information law was the development of the tort of misuse of private information from breach of confidence, under the influence of the Human Rights Act 1998 and Article 8 ECHR. This thesis considers that development in chapter 4 on the national implementation of European human rights, including how far the development was driven by the UK courts themselves or was driven by the ECHR and the Human Rights Act 1998.

Third, breach of confidence also developed state-facilitative and state-restrictive dimensions in relation to public authorities. Rather than existing in tension with market and individual approaches, these developments represent parallel specialised rules. These developments have created and sustained public-private divides in the law of confidentiality. The national courts were historically state-facilitative in their recognition of a public interest defence for the disclosure of confidential information to or by public authorities, where disclosure was reasonably connected with their functions, which were understood widely. The national courts also developed a set of state-facilitative duties of confidence to the Crown, imposed on ministers and certain officials to uphold institutions that supported the functioning of government, although state-restrictive assumptions also played a role in shaping those duties.[20] The national courts followed a state-restrictive approach by imposing duties of confidence on public authorities in relation to information gathered in the course of their functions, especially their coercive powers. In the 1990s this case law was itself tempered by the courts' state-facilitative approach to public interest disclosure or disclosure pursuant to statutory power.[21] In the most recent Supreme Court decision, however, the Supreme Court has made a dramatic move towards a state-restrictive approach, with the recognition of the confidentiality owed by public authorities is a fundamental common law right which necessitates the narrow interpretation of statutory powers to disclose such information.[22] The state-restrictive and state-facilitative approaches have therefore been in tension throughout the development of these doctrines. The law reflects some shifting tendencies between state-facilitative and state-restrictive approaches.

---

[19] See below, pp. 31 to 33.
[20] See below, pp. 39 to 43.
[21] The relationship between these two categories was sometimes unclear. See *Hellewell v Chief Constable of Derbyshire* [1995] 1 WLR 804, pp. 852 to 853; *Woolgar v Chief Constable of Sussex Police* [2000] 1 WLR 25, p. 36.
[22] *R (Ingenious Media) v Commissioners for Revenue and Customs* [2016] UKSC 54; [2016] 1 WLR 164.

CONFIDENCE AND COMMERCIAL RELATIONSHIPS: MARKET APPROACHES

Confidentiality at common law and in equity in the UK has long been informed by a market approach. This regulates market actors, irrespective of their status as public or private. The protection of confidentiality at common law and in equity has protected commercially valuable information, including information about individuals, from disclosure to support the functioning of the market. It has also protected the confidentiality between employer and employee, professionals and their clients, and fiduciaries and their principals in order to enable them to better carry out tasks of economic importance. For example, national courts have long protected confidentiality via implied contractual terms in contractual relationships.[23] Some of the relationships protected by breach of confidence were plainly commercial. The protection of confidentiality in those relationships served important market functions, such as supporting the relationship between banker or accountant and client.[24] This can also be seen in the national courts' treatment of fiduciary duties when using information gained in the course of fiduciary relationships.[25] These obligations contain no public-private divide and set a uniform level of regulation directed at enhancing the market.

In early cases, it was quickly established that the courts would protect confidentiality in a relationship of employment.[26] The courts also protected the confidentiality between certain professionals and their clients or customers. For example, in *Weld-Blundell v Stephens*, the court held that a chartered accountant must keep his client's letter of instruction confidential, even where the letter made libellous accusations.[27] Warrington LJ commented that there was "no reason founded on public policy or any other ground why an agent should be at liberty to disclose evidence of a private wrong committed by his principal".[28] The analysis was based on implied contractual terms. A similar analysis can be found in *Tournier v National Provincial and Union Bank of England*.[29] In that case, the court held that there was an implied contractual term that a banker would preserve his customer's confidence regarding "knowledge acquired in the character of a professional adviser" to him or her.[30] Banks LJ noted that the "credit of the customer depends very largely upon the strict

---

[23] See *Pollard v Photographic Co* (1888) 40 Ch D 345; *Weld-Blundell v Stephens* [1919] 1 KB 520; *Tournier v National Provincial and Union Bank of England* [1924] 1 KB 461. See also *Initial Services Ltd v Putterill* [1968] 1 QB 396.
[24] Weld-*Blundell v Stephens* [1919] 1 KB 520; *Tournier v National Provincial and Union Bank of England* [1924] 1 KB 461.
[25] *Boardman v Phipps* [1967] 2 AC 46.
[26] *Pollard v Photographic Co* (1888) 40 Ch D 345, p. 349.
[27] [1919] 1 KB 520.
[28] *Ibid.*, p. 535.
[29] [1924] 1 KB 461.
[30] *Ibid.*, p. 475.

observance of that confidence".[31] Scrutton LJ grounded his decision in implied terms "which must necessarily have been in the contemplation of the parties making the contract".[32] He had "no doubt" that such an implied term existed in relation to bankers and noted that it "applies in other confidential relations, such as counsel or solicitor and client, or doctor and patient."[33] Atkin LJ noted that the limit of the implied duty was reached where disclosure was "reasonably necessary for the protection of the bank's interests, either as against their customer or as against third parties in respect of transactions of the bank for or with their customer, or for protecting the bank, or persons interested, or the public, against fraud or crime".[34] These obligations preserve confidentiality in any information, including individual information, within commercial important relationships as a necessary part of their effective functioning and find their limit where the confidentiality would inhibit other commercial interests, including an economic interest in tackling fraud and other crime.

Some other traditional relationships of confidence, however, did not so obviously serve the market, such as doctor and patient or lawyer and client.[35] Confidentiality encourages frankness and the exchange of information between these vocations and the individuals they serve and so, in that sense, facilitate the "business" of a doctor, accountant, or lawyer. However, confidentiality also facilitates the access of individuals to professionals who serve a broader range of interests and rights, such as access to medical advice or treatment, with the benefits it brings to public health, or access to legal advice, as part of wider access to justice and in upholding the rule of law. The recognition of such relationships arguably reflects more an individual approach than a market one. It is difficult to characterise these relationships as purely commercial or intended to enhance the flow of information in the market. Rather, it is to protect individual privacy interests irrespective of the market. To that extent, individual and market approaches have coexisted and sometimes cooperated in the law of confidentiality from some of its earliest case law.

The market approach observed in the pre-1940s jurisprudence on confidence intensified in the late 1940s. From 1948, national courts developed clearer protection for commercial confidentiality in equity as well as through contractual interpretation. At this point, the law of confidence can be clearly distinguished as an independent field. *Saltman Engineering Co v Campbell Engineering Co* is often taken as the starting point for the modern law of breach of confidence.[36] In that case, Lord Greene held that the use of "confidential information",

---

[31] *Ibid.*, p. 474.
[32] *Ibid.*, p. 480.
[33] *Ibid.*, pp. 480 to 481.
[34] *Ibid.*, p. 480.
[35] *Ibid.*
[36] (1948) 65 RPC 203.

obtained "directly or indirectly" from the complainant and without the complainant's express or implied consent, would be a breach of confidence.[37] Such a principle, expressed at that level of generality, contained no public-private divide and reflected a market rationale. Various other cases subsequently dealt with misuse of commercial confidential information.[38] Injunctions were granted by the courts to prevent the continued use of information after a period of cooperation between businesses,[39] information obtained from the unlawful inspection of a hired telephone answering machine,[40] and confidential information about manufacturing processes.[41] This extended even to the unconscious use of confidential information.[42] A key concern was to prevent recipients of confidential information from using that information as a "spring-board" for activities detrimental to the economic interests of the confider.[43] In *Seager v Copydex*, Lord Denning MR expressed a "broad principle of equity that he who has received information in confidence shall not take unfair advantage of it".[44] He argued that one "should not get a start over others by using the information which he has received in confidence. At any rate, he should not get a start without paying for it".[45] This reflects market considerations about the economic value of information. Any protection of individuals was purely incidental to the market logic.

The conditions necessary for an obligation of confidence, outside a contractual relationship between the parties, were elaborated in 1969 by Megarry J in *Coco v AN Clark (Engineers) Ltd*.[46] The decision held that three conditions had to be fulfilled for a breach of confidence to occur: that the "information itself… [had] the necessary quality of confidence about it"; had "been imparted in circumstances importing an obligation of confidence"; and there had been "an unauthorised use of that information to the detriment" of the confider.[47] In that case, the confidential information had been exchanged for the purpose of a joint venture. However, the court held that an undertaking to pay royalties for the use of the information was sufficient instead of an injunction. Megarry J, discussing the "spring-board", considered that "the

---

[37] *Ibid.*, p. 213.
[38] *Nichrotherm Electrical Co Ltd v Percy* [1957] RPC 207; *Terrapin Ltd v Builders Supply Co (Hayes) Ltd* [1960] RPC 128; *Paul (Printing Machinery) Ltd v Southern Instruments (Communications) Ltd* [1964] RPC 118; *Bostitch Inc v McGarry and Cole Ltd* [1964] RPC 173; *Seager v Copydex Ltd* [1967] 1 WLR 923; *Suhner and Co AG v Transradio Ltd* [1967] RPC 329.
[39] *Terrapin v Builders Supply Co (Hayes)* [1967] RPC 375.
[40] *Paul (KS) (Printing Machinery) v Southern Instruments (Communications) and EP Ellis (Male) (t/a Ellis & Sons)* [1964] RPC 118.
[41] *Bostitch Inc v McGarry & Cole* [1964] RPC 173.
[42] *Seager v Copydex Ltd* [1967] 1 WLR 923; *Terrapin Ltd v Builders' Supply Co (Hayes Ltd)* [1967] RPC 375.
[43] *Terrapin Ltd v Builders Supply Co (Hayes) Ltd* [1960] RPC 128, 130; see also *Seager v Copydex Ltd* [1967] 1 WLR 923, p. 932.
[44] [1967] 1 WLR 923, p. 931.
[45] *Ibid.*, pp. 931 to 932.
[46] [1969] RPC 41.
[47] *Ibid.*, p. 419.

essence of the duty seems more likely to be that of not using without paying, rather than not using at all", where the duty related to the field of "industry and commerce".[48] Megarry J did, however, accept that that the "duty may exist in the more stringent form", that is not to disclose at all, outside the commercial context, such as *Argyll* confidentiality.[49] He insisted that the obligations in the commercial context must be those "upon which the same and fair conduct of business is likely to depend".[50] This extended to the question of whether to grant an injunction: "A product on the market may need protection against rivals in cases where a mere idea for a product, neither on the market now nor planned to be put on the market at any foreseeable date, may not".[51] The concerns of traditional confidentiality case law were therefore primarily commercial and market-orientated. Any protection for individual privacy that resulted from breach of confidence was incidental to this commercial logic grounded in a market approach. Further, there was no reason in principle why public authorities in appropriate circumstances could not be subject to such duties of confidence. The courts accepted that a more stringent approach could be found in order to protect certain information outside the commercial context: a rising individual approach. There was therefore little by way of a public-private divide in respect of such jurisprudence in the early jurisprudence of the national courts. A market approach dominated with some aspects of individual approaches coexisting or cooperating with that approach.

CONFIDENCE AND PRIVATE RELATIONSHIPS: INDIVIDUAL APPROACHES

Between the late 1960s and 1990s, before the important effects of the Human Rights Act 1998 were felt, the national courts nevertheless developed the law of confidentially according to an individual approach. This was not incompatible with parallel market approaches to commercial information and so in practice acted to extend protections and go beyond a market approach: an example of coexistence and transcendence of the market approach over time. This extended the recognition of non-commercial relationships as giving rise to duties of confidence and the eventual, though dicta, suggestion that "obviously confidential" information was protected per se by confidentiality.[52] This marked a stronger individual approach to confidentiality.

This expansion first recognised the marital relationship as such a relationship of confidence in 1967.[53] In *Argyll v Argyll*, one ex-spouse sought an injunction to protect information about

---

[48] *Ibid.*, p. 423.
[49] *Ibid.*; see below, p. 32.
[50] *Ibid.*, p. 425.
[51] *Ibid.*, p. 428.
[52] *Attorney General v Guardian Newspapers Ltd (No 2)* [1990] 1 AC 109.
[53] *Argyll v Argyll* [1967] Ch 302.

their "private life, personal affairs or private conduct communicated… during the subsistence of [the] marriage" from being disclosed to and by national newspapers.[54] The court expressly went beyond the clear principle that the "court may restrain any breach of confidence arising out of contract or any right of property"[55] to recognise that "the court in the exercise of its equitable jurisdiction will restrain a breach of confidence independently of any right at law."[56] These duties attached to the relationship and reflected an individual approach to confidentiality, building on top of the market approach of the earlier case law. The court considered that "there could hardly be anything more intimate or confidential than is involved in that relationship, or than in the mutual trust and confidences which are shared by husband and wife".[57] It also commented that "the confidential nature of the relationship is of its very essence and so obviously and necessarily implicit in it that there is no need for it to be expressed".[58] The court considered that the preservation of the confidentiality of marital communications was "an objective of public policy"[59] and the disclosures in question fell ""within the mischief which the law as its policy seeks to avoid".[60] No market interest was served by protecting such information. This shows the expanding influence of the individual approach, which entailed a greater level of protection for individuals, protecting their interests, but without a public-private divide. Any third party recipient of such confidential information could in principle be bound by it.

The courts subsequently went on to expand the categories of private relationship that would be protected by confidentiality. In *Francome v Mirror Group Newspapers*, information acquired via a press telephone tap was held to be subject to a duty of confidence.[61] In *Stephens v Avery*, a duty of confidence was recognised in relation to a friendship.[62] Information acquired by secret photography was held to be subject to a duty of confidence in *Shelly Films v Rex Features Ltd*[63] and *Creation Records Ltd v News Group Newspapers Ltd*.[64] Cases like *Barrymore v News Group Newspapers Ltd* extended duties of confidence to other sexual relationships.[65] The gradual extension of confidentiality to other relationships, and information acquired surreptitiously, marks the growing influence of an individual

[54] *Ibid.*, p. 318.
[55] *Ibid.*
[56] *Ibid.*, p. 332.
[57] *Ibid.*, p. 322.
[58] *Ibid.*
[59] *Ibid.*, p. 324.
[60] *Ibid.*, p. 330.
[61] [1984] 1 WLR 892.
[62] (1988) 11 IPR 439.
[63] [1994] EMLR 134.
[64] [1997] EMLR 444.
[65] [1997] FSR 600.

approach to the regulation of individual information through confidentiality law, developed by the courts.

Some dicta in the 1990s suggested that the courts would be willing to develop the law considerably to protect the confidential information of individuals. The dicta of Lord Goff in *Attorney General v Guardian Newspapers (No 2)* stated that a duty of confidence could:

> not merely to embrace those cases where a third party receives information from a person who is under a duty of confidence in respect of it, knowing that it has been disclosed by that person to him in breach of his duty of confidence, but also… an obviously confidential document… picked up by a passer-by.[66]

This is evidence that the law on confidentiality was already countenancing the protection of individual privacy long before the Human Rights Act 1998 came into force. Phillipson and Fenwick consider that, by covering "cases where obviously personal information is surreptitiously obtained",[67] the case law had already developed to a point at which it was "almost indistinguishable from a 'pure' privacy tort".[68] For Phillipson and Fenwick it was a "most radical development".[69] It certainly laid the ground for the later development of the law of confidence following the passage of the Human Rights Act 1998. It also demonstrates a willingness to protect far more than commercial confidences and business relationships necessary for the proper functioning of the market by 1990, indicating the growing influence of an individual approach in the development of the law of confidentiality transcending the market approach.

CONFIDENCE AND THE STATE: STATE-FACILITATIVE AND STATE-RESTRICTIVE APPROACHES

Any narrative that points only to the development of an individual model in the law of confidence would seriously neglect important counter tendencies, not least the tension between the state-facilitative and state-restrictive approaches in doctrines relating to public authorities. This is especially so in the more recent resurgence of a state-restrictive approach in the recognition of *Marcel* confidentiality as a common law fundamental right in R (*Ingenious Media) v Commissioners for Revenue and Customs*.[70]

---

[66] [1990] 1 AC 109, page 281.
[67] Gavin Phillipson and Helen Fenwick, *Breach of Confidence as a Privacy Remedy in the Human Rights Era* (2000) 63 MLR 660, 671.
[68] Phillipson and Fenwick (2000), p. 672; see also Andrew P Mackenzie, *Privacy – a New Right in UK Law?* (2002) Scots Law Times 98.
[69] Phillipson and Fenwick (2000), p. 670.
[70] [2016] UKSC 54; [2016] 1 WLR 154. See below, pp. 48 to 51.

Despite containing both market and individual approaches in the development of its jurisprudence, the national courts also showed a distinctive interest in state-facilitative and state-restrictive concerns when developing the law of confidentiality in relation to public authorities. The national courts did this in three respects. First, confidentiality adopted a relatively state-facilitative approach to the public interest defence in the context of disclosures to and by public authorities, at least initially. Second, the courts developed several duties of confidence owed by officials to the Crown and significantly shaped by the public context, reflecting a tension between state-facilitative and state-restrictive approaches. Third, the courts imposed duties of confidence on public authorities in relation to a wider range of information gathered through legal power or public duty, reflecting a state-restrictive concern but substantially tempered by state-facilitative attitude to statutory processing, at least until *Ingenious Media*.

PUBLIC AUTHORITIES AND THE PUBLIC INTEREST DEFENCE

Between the 1960s and 1990s, the national courts developed a public interest defence in the law of confidentiality in line with a state-facilitative approach. The national courts far more willingly and readily recognised an overriding public interest in the disclosure of confidential information by or to public authorities than to other private individuals or the general public. Only the press and medical professionals received similar treatment from the national courts, and sometimes only in more limited circumstances. However, this difference was later eroded as a growing focus on freedom of speech weakened the distinctiveness of the state-facilitative approach in national courts.

Early discussions concerning disclosure in the public interest emphasised the importance of disclosure "to one who has a proper interest to receive the information".[71] This was considered straightforward by the courts where there was a disclosure of "a crime to the police" or "a breach of the Restrictive Trade Practices Act to the registrar", although disclosure "on a broader field, even to the press" was accepted as at least excusable in some limited cases.[72] A defence of public interest in disclosing confidential information to the Daily Mail that revealed an employer to be misleading the public as to the reasons for price increases was not an unfounded defence, although this was not elaborated upon by the court in *Initial Services Ltd v Putterill*.[73] The stronger argument put to the court that the press was never a "proper authority" for the purpose of public interest disclosure was indeed

[71] *Initial Services Ltd v Putterill* [1968] 1 QB 396, p. 405.
[72] *Ibid.*, p. 406.
[73] *Ibid.*, pp. 405 to 407.

rejected by Salmon LJ.[74] However, neither was it endorsed with the same clarity and enthusiasm as a disclosure to the police. Disclosure to either public or private actors in the public interest was in principle possible. However, the jurisprudence took disclosure to public authorities for the purposes of their functions as clear examples, whereas disclosure to the press was merely excusable. This indicates a state-facilitative reasoning: a clear example of disclosure in the public interest is to the properly constituted public authority whereas less clear is the public interest in disclosure to the press or private organisations.

Another example can be found in *Butler v Board of Trade*.[75] The plaintiff tried to argue that confidential documents could not be adduced by the Board of Trade in legal proceedings. Goff J had no difficulty in holding that "the interest and duty of the defendants as a department of the state to prosecute offenders under the Companies Act must prevail over the offender's limited proprietary right in equity to restrain a breach of confidence".[76] It would be neither right nor permissible to exercise an equitable jurisdiction to restrain the prosecution from "adducing evidence relevant to the crime".[77] Disclosure to the proper public authority for the purposes of their functions was a clear and unproblematic public interest defence.

Similarly, in *Malone v Metropolitan Police Commissioner*,[78] although Sir Robert Megarry denied that a duty of confidentiality existed on the facts, he went on to consider whether there might be a public interest defence for breach of confidence by the police where the disclosure related not to wrongdoing, but the suspicion of wrongdoing.[79] Megarry VC said that the matter had to be approached with "some measure of balance and common sense".[80] Against the rights of telephone subscribers had to be balanced the "desires of the great bulk of the population" not to be victims of crime: such disclosures were "important weapons in protecting the public".[81] He held that the police would have "just cause or excuse",[82] a public interest defence, if there were "grounds for suspecting" individual telephone taps would give "material assistance in detecting or preventing crime", "discovering… criminals" or "otherwise assisting in the discharge of the functions of the police in relation to crime".[83] This would only apply if the material obtained was only used for those purposes.[84] Finally, any other

[74] *Ibid.*, p. 409.
[75] [1971] Ch 680.
[76] *Ibid.*, p. 691.
[77] *Ibid.*, p. 690.
[78] [1979] Ch 344.
[79] [1979] 1 WLR 760, pp. 376 and 377.
[80] *Ibid.*, p. 377.
[81] *Ibid.*
[82] *Ibid.*
[83] *Ibid.*
[84] *Ibid.*

irrelevant information acquired had to be restricted to the minimum number of people "reasonably required to carry out the process of tapping".[85] This dicta analysis suggests a state-facilitative approach to the public interest defence in 1979. This is because it was very comfortable with permitting disclosure to the police for the purpose of crime detection as a public interest.

Similarly, Scott J held, in *Re A Company's Application*,[86] that it was in the public interest for a financial and management advisor to disclosure those breaches of a regulatory scheme and tax improprieties "that it is the province of those authorities [Financial Intermediaries, Managers and Brokers Regulatory Association (FIMBRA) and the Inland Revenue] to investigate."[87] He considered that "no harm will have been done" if the regulator decided that "the allegations are not worth investigating" and "if harm is caused by the investigation itself, it is harm which is implicit in the regulatory role of [FIMBRA]".[88] Any confidential information would be information that the regulator was entitled to obtain pursuant to their powers.[89] Similarly, the disclosure of information relating to "fiscal matters that are the concern of the Inland Revenue" to the Inland Revenue would not breach confidentiality.[90] Again a clear state-facilitative approach influenced the public interest defence.

In *W v Egdell*,[91] the disclosure of a psychiatric report, which had been commissioned by a patient for a mental health tribunal appeal, but which was subsequently withdrawn by the patient after he saw the report, was held to be in the public interest where the disclosure was to the medical officer of the secure unit holding the patient and the Secretary of State. The patient suffered from paranoid schizophrenia and had killed a number of people with homemade bombs and other weapons. The commissioned report uncovered new evidence of ongoing dangerousness unknown to the secure unit. Sir Stephen Brown P held that the "balance of public interest clearly lay in the restricted disclosure of vital information to the director of the hospital and to the Secretary of State who had the onerous duty of safeguarding public safety".[92] Once again the national courts facilitated the flow of information to public authorities charged with public functions, although it was not considered whether such information could be disclosed directly to other parties for their safety.

---

[85] *Ibid.*
[86] [1989] Ch 477.
[87] *Ibid.*, p. 483.
[88] *Ibid.*, p. 482.
[89] *Ibid.*
[90] *Ibid.*
[91] [1990] Ch 359.
[92] *Ibid.*, p. 416.

The national courts also distinguished the wholly commercial context from the context of public authority functions in *Re Smith Kline and French Laboratories*.[93] In doing so it emphasised that the public interest in disclosure to a public authority exercising public functions might be privileged. In that case a company provided confidential information to a licensing authority under the Medicines Act 1968 in order to obtain a licence for their product. They did not wish their information to be used for other purposes or to benefit their competitors. Licences could be obtained by competitors who showed that their product was "essentially similar" to an existing licenced product. The company applied for judicial review to prevent the licensing authority's proposed use of their information to evaluate competitors' applications for licences as "essentially similar" products because this would entail using or disclosing their confidential information to competitors. The fact that a product was ruled "essentially similar" could be valuable information to a competitor. Dillon LJ held that the court had to take a "practical approach"[94] and that because the licensing authority was "a public authority exercising important functions in the public interest" the resolution of the case would not necessarily "be the same as it might have been in *a wholly commercial context*", a clear state-facilitative consideration.[95] He held that because the "protection of public health is the fundamental purpose of the licensing system" under the relevant Act and a "purpose of great public importance".[96] The authority could therefore use the information for all its statutory functions.[97] No more granular assessment of the public interest was undertaken. The case shows a clear state-facilitative tendency within the jurisprudence on public interest defences, explicitly distinguishing it from the same test in a wholly commercial context.

Public interest defences were readily found for the disclosure of confidential information to public authorities between the 1960s and 1990s, especially where they had responsibilities relating to crime, regulation or public safety. A public interest analysis was also later applied to the disclosure of confidential information held by public authorities themselves.[98] A state-facilitative approach is apparent in this when this is compared to the public interest defence for the disclosure of confidential information to private actors. The public interest defence could be relied on by individuals disclosing confidential information to private actors, but in more limited circumstances.

---

[93] [1990] 1 AC 64.
[94] *Ibid.*, p. 75.
[95] *Ibid.*, p. 80.
[96] *Ibid.*, p. 81.
[97] *Ibid.*, p. 82.
[98] See below, pp. 46 to 47.

In 1969 in *Fraser v Evans*,[99] Lord Denning MR, in obiter dicta comments, considered that some matters "are of such public concern that the newspapers, the Press, and indeed, everyone is entitled to make known the truth and to make fair comment on it" as "an integral part of the right to free speech and expression", which "must not be whittled away".[100] Similarly, in *Hubbard v Vosper*,[101] Lord Denning MR held that confidential disclosure of materials from a Scientology course could potentially be published in the public interest where the relevant courses "contain such dangerous material that it is in the public interest that it should be made known."[102] This judgment was followed in similar circumstances in *Church of Scientology v Kaufman* by Goff J.[103] The public interest defence was therefore also available in principle for disclosure to private actors.

However, the public interest defence was initially relatively narrow. In *Beloff v Pressdram*,[104] Ungoed-Thomas J held that the reproduction of an internal Observer memorandum describing a conversation between the plaintiff and a named Cabinet Minister was subject to public interest defence only in relation to completed or contemplated "breach of the country's security… 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 misdeed of similar gravity.[105] Contrast that with the acceptance of the public interest in wide use and disclosure by a public authority for the better performance of all its statutory functions in *Re Smith Kline and French Laboratories*.[106] The court held that because the memorandum in question failed to disclose "any 'iniquity' or 'misdeed'", it fell outside the scope of the public interest defence.[107] This was narrower than disclosure to public authorities for their functions.

On the other hand, some cases became considerably more liberal in their approach to public interest disclosures. The jurisprudence was not consistent over time. There is some evidence that the expansion of public interest defences to enhance free speech eroded the public-private divide. In *Woodwood v Hutchins*,[108] Lord Denning MR held that the public interest permitted the disclosure of confidential information by a press relations agent to the press relating to several singers following the termination of the contract between them. This

---

[99] *Fraser v Evans* [1969] 1 QB 349.
[100] *Ibid.*, p. 363.
[101] [1972] 2 QB 84.
[102] *Ibid.*, p. 96.
[103] [1973] RPC 627, pp. 596 and 599.
[104] [1973] FSR 33.
[105] *Ibid.*, p. 57.
[106] See above, p. 37.
[107] [1973] FSR 33, p. 58.
[108] [1977] 1 WLR 760.

was done to correct a false image cultivated by those singers in the press.[109] Lord Denning MR held that the singers had "sought publicity" and presentation "in a favourable light" to their commercial advantage, and could not subsequently complain "if a servant or employee of their afterwards discloses the truth about them" because "the image which they fostered was not a true image". It was therefore "in the public interest that it should be corrected."[110] He considered that "there should be truth in publicity. The public should not be misled".[111] In *Schering Chemicals Ltd v Falkman Ltd*, Lord Denning also emphasised the importance of press freedom and the public interest defence.[112] He held that it should only be restricted where there was a "social need for protecting the confidence sufficiently pressing to outweigh the public interest in freedom of the press" and "where the private interest in maintaining the confidence outweighs the public interest in making the matter known to the public at large".[113] Later, in *Lion Laboratories v Evans*,[114] the court held that it was in the public interest for former employees of a manufacturer of breathalyser instruments to supply confidential information relating to the inaccuracy of such instruments to a newspaper, expanding the public interest defence to circumstances where there was no wrongdoing on the part of the plaintiffs.[115] Stephenson LJ did not doubt the "right of the press to probe and question", although he did still "doubt that technical matters… [were] best investigated in the columns of a daily newspaper" rather than the Home Office.[116] Although initially disclosure to or by public authorities for functions related to criminal investigation, regulatory, public safety, and even the efficient exercise of licensing powers, were readily accepted by the courts, reflecting state-facilitative tendencies, this was somewhat eroded by the development of public interest defences, as these expanded to address freedom of speech concerns. Nevertheless, the earlier history of public interest defences in confidentiality law demonstrate a state-facilitative approach to public authorities.

Duties of Confidence to the Crown

Alongside other equitable duties of confidence imposed on individuals in certain relationships, in the mid-1970s the national courts developed a set of obligations of confidence on Cabinet ministers and certain other officials. These obligations had an unusual public character and operated distinctively from general equitable obligations of confidence, reflecting the fact that they were owed to the Crown and not to the individuals

---

[109] *Ibid.*, p. 764.
[110] *Ibid.*, pp. 763 to 764; see also p. 765, per Bridge LJ.
[111] *Ibid.*, p. 764.
[112] [1982] QB 1.
[113] *Ibid.*, p. 23.
[114] [1985] QB 526.
[115] See *Ibid.*, p. 550, per Griffiths LJ.
[116] *Ibid.*, p. 535.

involved in their private capacity. These distinctive aspects reflect a hybrid of state-facilitative and state-restrictive tendencies. They were state-facilitative in that the obligation was imposed to facilitate government and to centralise processes for the authorisation of disclosure. However, they contained state-restrictive elements which denied the state a free-standing interest in confidentiality and insisted on injunctive relief only where it was in the public interest to have it.

In 1976, in *AG v Jonathan Cape*,[117] Lord Widgery CJ held that the obligation of secrecy that attached to Cabinet discussions was not merely binding in morals but also in law.[118] He denied that the courts were "powerless to restrain the publication of public secrets, while enjoying the *Argyll* powers in regard to domestic secrets"[119] and that "when a Cabinet Minister receives information in confidence the improper publication of such information can be restrained by the court."[120] This followed from the fact that the doctrine of collective Cabinet responsibility was "an established feature of the English form of government" so that "some matters leading up to a Cabinet decision may be regarded as confidential."[121] This duty of confidence demonstrated an unusual public character. It was not merely the recognition of a conventional private duty of confidence. A conventional duty of confidence might be expected to apply to the recipient of confidential information in Cabinet and be owed to the minister who imparted the information in confidence. Rather, the shape of the duty was distinctively public. Lord Widgery CJ explained that as the duty was "imposed to enable the efficient conduct of the Queen's business" it was the case that "the confidence is owed to the Queen and cannot be released by the members of Cabinet themselves".[122] First, the imposition of a duty to enable efficient government business expresses a state-facilitative approach to the regulation of such information. Second, it was not a legal right of the individual who expressed the confidential information. It was explicitly not like ordinary duties of confidence between private individuals, whose own consent to disclosure would be sufficient. Instead, Widgery CJ elaborated that "a resigning Minister who wishes to make a personal statement in the House, and to disclose matters which are confidential under the doctrine obtains the consent of the Queen" and that consent is "obtained through the Prime Minister".[123] This approach to consent for the purposes of confidentiality mirrored the constitutional convention regarding Cabinet responsibility. The effect of the duty was therefore to concentrate decision-making authority in the hands of the Prime Minister,

---

[117] [1976] QB 752.
[118] *Ibid.*, p. 767
[119] *Ibid.*, pp. 769 to 670.
[120] *Ibid.*
[121] *Ibid.*
[122] *Ibid.*
[123] *Ibid.*

providing control over the disclosure of confidential Cabinet discussions. Furthermore, Widgery CJ held that he could not "accept the suggestion that a Minister owes no duty of confidence in respect of his own views expressed in Cabinet".[124] The duty therefore not only could not be released by the confider, but it also acted to bind the confider him or herself, completely unlike ordinary duties of confidence. Widgery CJ's justification for this was that otherwise the confidence, needed for the efficient conduct of Government business, could too readily be undermined: "It would only need one or two Ministers to describe their own views to enable experienced observers to identify the views of the others.[125] The result was a highly unusual duty shaped by a state-facilitative approach.

However, the new duty also contained some state-restrictive dimensions showing a mixture or tension of approach. The duty of confidence in *Attorney General v Jonathan Cape* did not give rise to remedies *per se* but could only be protected by an injunction in more limited circumstances. A breach could only be "restrained by the court when this is clearly necessary in the public interest."[126] This was quite different from the duties of confidence owed to private individuals, who have remedies against a breach unless a public interest defence applies. Instead, the effective burden was reversed, so that the Crown must show a public interest in restraining publication. This is a state-restrictive dimension because it denies the state free-standing interests in confidentiality which it can enforce against third parties. Instead, the state must point to reasons beyond its own interest to restrain the disclosure of confidential information. Such a limitation is state-restrictive in nature.

In 1990, the House of Lords in *Attorney General v Guardian Newspapers Ltd (No 2)*[127] imposed a similar duty of confidence to the Crown on members of the security service.[128] Lord Keith commented that the disclosure of confidential information could "result in a financial loss to the public" or "tend to harm the public interest by impeding the efficient attainment of proper government ends".[129] Commenting on the distinctively public nature of the duty being recognised in equity, Lord Keith said that "the position of the Crown, as representing the continuing government of the country may… be regarded as being special".[130] This was because the Crown "representing the nation as a whole" had "no private life or personal feelings capable of being hurt by the disclosure of confidential

---

[124] *Ibid.*
[125] *Ibid.*
[126] *Ibid.*, p. 771.
[127] [1990] 1 AC 109.
[128] See also *Lord Advocate v The Scotsman* [1990] 1 AC 812, p. 818.
[129] [1990] 1 AC 109, p. 256.
[130] *Ibid.*

information".[131] Therefore, the Crown could only seek "to prevent disclosure or to seek redress" if it was "in a position to show that the disclosure is likely to damage or had damaged the public interest".[132] Lord Keith stated that what must be shown by the Crown would "depend on the circumstances of each case".[133] He accepted that there might be a "general public interest in the preservation of confidentiality" owed by Crown servants and their agents and "in encouraging other Crown servants to preserve it".[134] He noted that the "position may be different" in a case "where publication is proposed by third parties unconnected with the particular confidant".[135] The suggestion seems to be that in relation to the public interest, an injunction may be granted more readily to prevent breach by a Crown servant or agent than by a third party who obtains confidential information with knowledge from such a person. A state-restrictive logic therefore runs through this part of the law of confidentiality, tempering the state-facilitative approach underpinning the doctrine. This was later applied in *Lord Advocate v The Scotsman*.[136] In that case the concession that further publication would not be capable of damaging national security, such that the contents of a book written by a former member of MI6 was "entirely innocuous", led the court to hold that no prima facie claim for breach of confidence could be pleaded.[137] Lord Jauncey noted that it was "now beyond doubt that the Crown can only restrain the publication of confidential information if the public interest requires such restraint."[138]

The courts have, on the other hand, also shown a willingness to go even further to enforce duties of confidence against former members of the security services than against private parties: a state-facilitiative approach. In *Attorney General v Blake*,[139] the court held that, despite the disclosure of information in a book by the double agent George Blake no longer being confidential nor damaging to the public interest by 1989,[140] it would enforce the contractually binding confidentiality undertaking of the defendant[141] by an account for profits, considering the case to be an exceptional one where other remedies were "inadequate".[142] Lord Nicholls added that the "Crown had and has a legitimate interest in preventing Blake profiting from the disclosure of official information, whether classified or not, while a member

---

[131] *Ibid.*
[132] *Ibid.*
[133] *Ibid.*
[134] *Ibid.*
[135] *Ibid.*
[136] [1990] 1 AC 812.
[137] *Ibid.*, p. 819.
[138] *Ibid.*, p. 828.
[139] [2001] 1 AC 268.
[140] *Ibid.*, p. 275.
[141] *Ibid.*, p. 277.
[142] *Ibid.*, p. 285.

of the service and thereafter."[143] This was to remove the "financial incentive" from members of the security service to break their undertaking and because the "undertaking, if not a fiduciary obligation, was closely akin to a fiduciary obligation, where an account of profits is a standard remedy in the event of breach… In the special circumstances of the intelligence services, the same conclusion should follow even though the information is no longer confidential."[144] Although in highly unusual circumstances, the case reflects a state-facilitative concern to protect the confidentiality of security services information. The courts have been willing to remove the financial incentive to leak official information, even where it was no longer confidential due to the passage of time. Within the special duties of confidence owed to the state, both state-facilitative and state-restrictive approaches have interacted to shape legal doctrine.

Duties of Confidence of Public authorities to Private Actors

In the 1990s, the scope and nature of duties of confidentiality owed by public authorities to private actors was significantly developed by the courts. This was done according to a state-restrictive approach, although exceptions were heavily influenced by the legislative context, which acted in a broadly state-facilitative manner.

One core historic limitation on the law of confidentiality was its inability to impose duties of confidence on public authorities. This was due to the common lack of a contract into which to imply duties of confidence on a public authority, in contrast to the common presence of a contract between private individuals.[145] The effect of this reliance on implied terms in contract was initially to facilitate the state. This was illustrated clearly in *Malone v Metropolitan Police Commissioner*.[146] Although a claim based upon confidentiality failed in relation to the interception of telephone conversations on the authority of warrants issued by the Secretary of State, Sir Robert Megarry also noted that had the telephone services in question been provided under a contract with the Post Office, then an argument based on implied terms might have been feasible.[147] Such an implied term would provide that the "telephone conversations should remain confidential and be free from tapping".[148] However, the effect of the statutory regime was that telephone services were provided pursuant to a statutory duty, with a statutory power to "make a scheme of charges and other terms and

[143] *Ibid.*, p. 287.
[144] *Ibid.*
[145] See above, p. 28.
[146] [1979] Ch 344.
[147] *Ibid.*, p. 375.
[148] *Ibid.*

conditions for those services" with those charges recoverable as if "simple contract debts".[149] This meant that that "no contract as such" existed between the public body and the individual and so no "contention based on implied terms" was possible.[150] There was therefore no implied contractual duty binding on the public authority in question. Had the service provider been a private actor, reliant on a contract for services, then such a duty could have been implied. The fact that the relevant service was carried out under statutory power rather than contract therefore undermined the ability of the national court to impose an implied term concerning the confidentiality of the telephone service. This would often be the case where public authorities provided services pursuant to statute rather than through contract. The operation of the law was therefore state-facilitative.

The courts were also initially resistant to attempts by private actors to impose duties of confidence on public authorities by seeking to make confidential disclosures to such public authorities. In *Re Smith Kline and French Laboratories*,[151] the court held that the licensing authority could use the confidential information disclosed to them for any purpose of the Act and not just the single purpose for which the company had disclosed it in the original application. In addition to resting this on a public interest analysis,[152] Lord Templeman suggested that the company could only provide the information to the public authority on the basis that it was "for the *purposes* of the Act"[153] and not for more limited purposes. This created an all or nothing approach to confidential disclosures based on the total scope of the authority's powers. It did not permit a more limited disclosure for a defined purpose. This would be possible in relation to confidential disclosures to private bodies. Lord Templeman explained that this was "the price which the appellants must pay for cooperating in the regime designed by Parliament for the protection" of others.[154] In the Court of Appeal, Staughton LJ had contrasted exchanges between private parties where it "may be possible to discern a common purpose for entrusting information", with disclosure to a public authority where "the purpose is less likely to be common" to the parties.[155] In those cases, the "purpose of the licensing authority in acquiring the information was to use it for *all or any of its duties*" was determinative of the purposes for which the information could be used.[156] Therefore, there was no need to consider "any countervailing public interest" to justify such

[149] *Ibid.*
[150] *Ibid.*
[151] [1990] 1 AC 64.
[152] See above, pp. 34 to 39.
[153] [1990] 1 AC 64, p. 104 (emphasis added).
[154] *Ibid.*
[155] *Ibid.*, p. 89.
[156] *Ibid.*, pp. 89 to 90 (emphasis added).

use.[157] In effect, information provided to public authorities would be for all their lawful functions. This involved a state-facilitative approach to public authorities going even beyond public interest defences. The existence of a statutory purpose precluded any further analysis of the public interest.

In the 1990s, the national courts' jurisprudence started to reflect a more state-restrictive model in relation to information provided to public authorities. The national courts did this by subjecting information disclosed to public authorities under compulsion to a duty of confidence. However, the operation of exceptions for disclosures pursuant to statutory or other powers, or a public interest defence highly deferential to the statutory scheme, in effect rendered the scope of this duty of confidence coterminous with the public authority's powers, broadly understood. This meant that the use of such information for those powers was permitted. Only ultra vires disclosure was a breach of confidence. This increased the remedies available to individuals against public authorities for unlawful disclosure of such information: a state-restrictive approach to public authority use of information acquired pursuant to public power. However, the law remained relatively state-facilitative where a public authority used information within the scope of its powers. Therefore both state-facilitative and state-restrictive tendencies operated within this area of the law of confidentiality.

In *Marcel v Metropolitan Police Commissioner*,[158] police released documents that had been seized during a criminal investigation to solicitors who wished to bring a civil action. This was done before a subpoena had been properly served on the police. Dillon LJ held that "powers to seize and retain [documents] are conferred for the better performance of *public* functions by *public bodies* and cannot be used to make information available to *private* individuals for their *private* purposes".[159] This meant that the "police should not disclose documents, otherwise than for the specific purposes specified in the [relevant legislation], unless a subpoena had been served on the relevant police officer."[160] The documents and information seized during a police search were confidential and could only be used for the performance of public functions or disclosed pursuant to an order of the court. Dillon LJ observed that "because the police officer seizes documents under the [relevant legislation] for limited purposes… he owes a duty of confidence to the owner not to use the documents for other purposes".[161] Sir Christopher Slade emphasised the "draconian" nature of search and seizure powers and the expectation "that the authority would treat the documents and

[157] *Ibid.*
[158] [1992] Ch 225.
[159] *Ibid.*, pp. 256 to 257.
[160] *Ibid.*, p. 258.
[161] *Ibid.*, p. 257.

their contents as confidential, save to the extent that it might use them for purposes as contemplated by the relevant legislation".[162] The emphasis on the limited purposes for which public authorities could act and the coercive nature of the collection of that information justified the decision. This is a state-restrictive approach.

The *Marcel* doctrine was subsequently extended beyond information obtained through draconian police powers. In *Hoechst UK Ltd v Chemiculture Ltd*,[163] Morritt J applied *Marcel* to information which had been disclosed by an officer of the Health and Safety Executive. The information had been obtained by the exercise of powers conferred by the Food and Environment Protection Act 1985. The powers were wider than powers of search and seizure. Morritt J held that "information obtained pursuant to statutory powers can only be disclosed by the recipient to such persons and for such purposes as are envisaged by the statute conferring the powers or pursuant to a court order".[164] *Marcel* confidentiality was therefore expanded to a wider application, covering information obtained through the exercise of statutory power. With this, the state-restrictive approach expanded to cover considerably more information.

In subsequent cases, it became unclear whether the *Marcel* principle permitted any disclosures pursuant to a legal power or whether the statutory context was informative but not exhaustive of the public interest in disclosure. There were therefore two different lines of case law, the latter potentially more state-facilitative than the former. First, in *Re Arrows (No 4)*,[165] the court took the former approach. It considered whether information given to the liquidators of a company could be disclosed to the Serious Fraud Office. Lord Browne-Wilkinson held that "the *Marcel* principle cannot operate to prevent the person obtaining the information from disclosing it to those persons to whom the statutory provisions either require or authorise him to make disclosure" before noting that the relevant Act contained a "series of provisions which envisage that information and documents in the hands of the liquidators is to be disclosed to others, including disclosure for the purposes of criminal 'proceedings'."[166] The national courts therefore allowed statutory powers to override Marcel confidentiality without more.[167] In some later cases, on the other hand, the tendency to align duties of confidence with the relevant statutory framework was displaced by a more liberal public interest. In *Hellewell v Chief Constable of Derbyshire*,[168] the court held that the

[162] *Ibid.*, p. 262.
[163] [1993] FSR 270.
[164] *Ibid.*, p. 277.
[165] [1995] 2 AC 75.
[166] *Ibid.*, p. 102.
[167] *Ibid.*, p. 99.
[168] [1995] 1 WLR 804.

release of a custody photograph of a known shoplifter to shop employees was not a breach of confidence. Laws J held on that on general principles, and based on *Marcel*, that a suspect photograph was confidential information.[169] Laws J held that the police could "make reasonable use" of a photograph "for the purpose of the prevention and detection of crime, the investigation of alleged offences and the apprehension of suspects or persons unlawfully at large".[170] Laws J suggested that the "better analysis" of this lay in the public interest defence.[171] The action by the police had been "obviously and unarguably in the public interest" as it had been "reasonably directed to the prevention of crime."[172] Similarly, in *Woolgar v Chief Constable of Sussex Police*,[173] the court considered whether the police could disclose a police interview transcript without the suspect's consent to the regulatory body for nursing. The transcript was straightforwardly confidential.[174] Kennedy LJ held that where a regulatory body which was held to be "operating in the field of public health and safety" sought access to information and the police were "reasonably persuaded [that it] is of some relevance to the subject matter of an inquiry being conducted by the regulatory body", this would give rise to a "countervailing public interest" which would entitle "the police to release the material to the regulatory body on the basis that, save in so far as it may be used by the regulatory body for the purposes of its own inquiry, the confidentiality which already attaches to the material will be maintained."[175] Kennedy LJ added that even in the absence of a request the police could pass on confidential information which "in their reasonable view" was "in the interests of public health or safety".

In both *Hellewell* and *Woolgar*, the courts analysed disclosure based on the reasonable view of the public authority that disclosure would be in the interests of the public functions of their own or another public authority, as a public interest defence. This was sometimes wider, and therefore more state-facilitative, than the narrower approach in *Re Arrows (No 4)*. However, in either line of case law the effect of these authorities was to establish state-facilitative exemptions for disclosure in the pursuit of public functions. The duty itself was state-restrictive to the extent it granted remedies to individuals for unlawful disclosure which did not exist under *Malone v Metropolitan Police Commissioner* and could not be implied in the public authority context due to the frequent absence of a relevant contract. The development of the *Marcel* doctrine therefore shows a mixture of state-facilitative and state-restrictive approaches to the public-private divide.

---

[169] *Ibid.*, p. 810.
[170] *Ibid.*
[171] *Ibid.*, pp. 810 to 811.
[172] *Ibid.*, p. 811.
[173] [2000] 1 WLR 25.
[174] *Ibid.*, p. 29.
[175] *Ibid.*, p. 36.

R (INGENIOUS MEDIA) V COMMISSIONERS FOR REVENUE AND CUSTOMS

In the most recent case law, the Supreme Court has taken a more state-restrictive approach to confidentiality. It did this by recognising *Marcel* confidentiality as a common law fundamental right in the context of interpreting the scope of statutory powers to disclose confidential information. The result of this was that the principle of legality applies to statutory powers to disclose confidential information, potentially narrowing the interpretation of exemptions to *Marcel* confidentiality. This represents a shift in the balance between state-facilitative and state-restrictive approaches in the most recent thinking of the UK Supreme Court, towards the latter.

In *R (Ingenious Media) v Commissioners for Revenue and Customs*,[176] the Permanent Secretary for Tax at Her Majesty's Revenue and Customs (HMRC) disclosed information, in an off-the-record meeting, to journalists. The information related to the tax activities of the applicants, who were involved in film investment schemes, and HMRC's view of those activities. This was all information derived from information held by HMRC in connection with its functions. Some of the information was later published in a national newspaper. The case was brought as a judicial review, seeking a declaration, rather than as an action for breach of confidence. HMRC officials were bound by a statutory duty of confidentiality in section 18(1) of the Commissioners for Revenue and Customs Act 2005. That duty extended to "information which is held by the Revenue and Customs in connection with a function of the Revenue and Customs". Exemptions to the statutory duty were listed in section 18(2). The case concerned the proper interpretation of section 18(2)(a)(i), which provided an exemption for disclosures "made for the purposes of a function of the Revenue and Customs". The Permanent Secretary for Tax argued that the practice of off-the-record meetings with journalists covering financial news, involving limited disclosures was for the purposes of a function of HMRC. This was because such disclosures brought HMRC several benefits: the meetings encouraged good relations with the press, enabled HMRC to more effectively communicate its approach to complicated tax avoidance schemes to the public, and provided opportunities for investigative journalists to share information with HMRC about individuals that might help HMRC in its own investigations.

The High Court and Court of Appeal both treated the case as a conventional judicial review. They both held that the disclosure was a proper one under section 18(2)(a)(i). Sales J, in the High Court,[177] held that there was a "rational connection between the function of HMRC to

[176] [2016] UKSC 54; [2016] 1 WLR 164.
[177] *R (Ingenious Media) v Commissioners for Revenue and Customs* [2013] EWHC 3258 (Admin).

collect tax in an efficient and cost-effective way" and the disclosures in question.[178] The Permanent Secretary for Tax had made a "judgment" that "fell within the lawful parameters" of section 18(2).[179] This was because the decision required "evaluative judgments".[180] It was inappropriate for the "court to approach the matter as if it were the primary decision-maker" because the court was not "deeply familiar" with the "background of policy" and press relations, whereas the Permanent Secretary for Tax and his advisers were "experts".[181] It was "legitimate" to seek good press relations and the decision was one "properly and rationally" open to the Permanent Secretary for Tax.[182] In the Court of Appeal,[183] Sir Robin Jacob favoured a "wide view" of permissible disclosure.[184] The court was not "a tax gatherer" nor "in a position to evaluate the likely effect of a disclosure on an HMRC function in the same way as an official concerned with the day to day operation of the system".[185] He ultimately concluded that it was "entirely in the public interest that HMRC should let the public know its views about [film investment schemes]".[186] The decisions of the High Court and Court of Appeal were therefore relatively state-facilitative: imposing low intensity review out of deference to the expertise of the authority and generous in interpreting the functions of HMRC to include efficiency and cost-effectiveness. In this, they were deferential to the decision of the Permanent Secretary, holding that a decision to disclose was an evaluative judgment. The decisions held that the disclosures were also proportionate interferences with both Article 8 ECHR and Article 1 Protocol 1 ECHR.

The Supreme Court took a much more state-restrictive approach to the disclosures. It rejected the wide interpretation of section 18(2)(a)(i) favoured by the High Court and Court of Appeal. The Supreme Court decision differed from the earlier judgments by drawing on the *Marcel* jurisprudence. It did not merely reflect a difference is opinion about the appropriate scope of the statutory exemption or the proper degree of deference to the decision-maker. Rather, Lord Toulson identified *Marcel* as authority for a "well-established principle of the law of confidentiality that where information of a personal or confidential nature is obtained in the exercise of a legal power or in the furtherance of a public duty, the recipient will in general owe a duty to the person from who it is received or to whom it relates not to use it for other

[178] *Ibid.*, para. 39.
[179] *Ibid.*
[180] *Ibid.*, para. 40.
[181] *Ibid.*
[182] *Ibid.*, paras 43 to 46.
[183] *R (Ingenious Media) v Commissioner for Revenue and Customs* [2015] EWCA Civ 173; [2015] 1 WLR 3183.
[184] *Ibid.*, para. 29.
[185] *Ibid.*, para. 46.
[186] *Ibid.*, para. 71.

purposes".[187] In particular, Lord Toulson did not focus on the statutory confidentiality imposed by section 18(1). Lord Toulson's judgment emphasised those parts of the earlier case law that characterised statute as overriding confidentiality, rather than a public interest analysis: the narrower of the two lines of cases law. He cited *In Re Arrows (No 4)*[188] as authority for the proposition that *Marcel* confidentiality could not prevent disclosures either required or authorised by statute. The judgment did not refer to *Hellewell* or *Woolgar*, where the public interest analysis was shaped by the statutory context and was arguably broader.

Lord Toulson subjected the broader interpretation of section 18(2)(a)(i) to a more fundamental set of criticisms. He argued that were section 18(2)(a)(i) to be interpreted broadly, then the obligation of *Marcel* confidentiality owed by HMRC would "have been very significantly eroded by words of the utmost vagueness".[189] The principle of legality applied, as articulated by Lord Hoffman in *R v Secretary of State for the Home Department, Ex p Simms*: "Fundamental rights cannot be overridden by general or ambiguous words".[190] The Supreme Court therefore held that a *narrower interpretation* of section 18(2)(a)(i) must be adopted, limiting disclosure to the purpose of HMRC's primary function of revenue management and collection. Lord Toulson emphasised that "public bodies are not immune from the ordinary application of the common law".[191] The Supreme Court judgment is a significant development in the *Marcel* jurisprudence, requiring narrower interpretations of statutory powers to use confidential information because *Marcel* confidentiality is a fundamental common law right.

Daly welcomed the Supreme Court judgment for "bringing clarity"[192] and observed that:

> When it comes to protecting rights, the courts jealously guard the individual against the state. The history of the British Constitution is replete with examples of judges scrupulously examining the precise intention of Parliament when it gives powers to public officials which purport to override individual liberties.[193]

This is certainly true and reflects a long tradition in UK constitutional law.[194] However, seen in the light of the earlier case law on *Marcel* confidentiality, it is questionable whether this

---

[187] [2016] UKSC 54; [2016] 1 WLR 164, para. 17.
[188] [1995] 2 AC 75.
[189] [2016] UKSC 54; [2016] 1 WLR 164, para. 19.
[190] [2000] 2 AC 115.
[191] [2016] UKSC 54; [2016] 1 WLR 164, para. 28.
[192] Stephen Daly, *R (Ingenious Media) v HMRC: Public Disclosures and HMRC's Duty of Confidentiality* (2017) British Tax Review 10, 19.
[193] *Ibid.*, pp. 13 to 14.
[194] See, for example, *Entick v Carrington* 95 ER 807.

really was an orthodox application of *that* "well-established principle".[195] The Supreme Court took a far more state-restrictive approach to *Marcel* confidentiality than the courts did in the 1990s. It represents an important development of the jurisprudence on confidentiality on the part of the Supreme Court and demonstrates a resurgence and strengthening of the state-restrictive approach in this field and an expansion of the fundamental rights recognised and protected in the common law.

THE PUBLIC-PRIVATE DIVIDE IN CONFIDENTIALITY

The history of confidentiality in common law and equity demonstrates the importance of the four-approach framework for analysing the development of the public-private divide in individual information law. Early case law on confidentiality emphasised implied terms, fiduciary and commercial relationships and the protection of information to enhance the market. It had no public-private divide and was more limited in its scope, protecting information and relationships necessary to promote business and commercial interests. Even at a relatively early stage, long before the influence of the Human Rights Act 1998, the law showed a tendency to expand beyond the limits of a market rationale to increasingly protect information and relationships that vindicated the privacy of the individual. Regarding an expanding set of relationships, an individual approach transcended the wider market approach in the law of confidentiality. Although neither of these legal developments contained a public-private divide, they ran parallel to several lines of case law that applied the law of confidentiality distinctively in relation to public authorities from the 1960s. Although both state-facilitative and state-restrictive elements were present in specialised parts of the law on breach of confidence, the most recent judgment of the Supreme Court reflects a later turn towards a state-restrictive approach to information gathered pursuant to legal power or public duty. The recognition of *Marcel* confidentiality as a fundamental right demonstrates the ongoing importance of state-restrictive approaches. The history of confidentiality reveals complex interactions between different approaches to the public-private divide. It provides a more complex picture than the expectation of a linear progression towards an individual model. Beyond struggle, these interactions show parallel development, coexistence, cooperation and shifts in emphasis over time.

---

[195] See, for further discussion, Oliver Butler, *Confidentiality and Public Authorities: Fundamental Rights, Legality and Disclosure for Statutory Functions* (2017) 76(2) CLJ 253.

CHAPTER 3

THE PUBLIC-PRIVATE DIVIDE AND EUROPEAN HUMAN RIGHTS

INTRODUCTION

European human rights law, binding on the UK as a matter of international law, was a major European influence on the development of the public-private divide in UK individual information law. This chapter examines how the public-private divide developed in relation to the right for respect for private life in Article 8 of the European Convention on Human Rights (ECHR). It demonstrates the role of various actors and approaches in the development of that divide and, although an individual approach has undoubtedly risen in prominence, it also demonstrates the resurgence of state-restrictive approaches and the endurance of limited state-facilitative elements.

The history of the right to respect for private life in Article 8 ECHR demonstrates the rise of an individual approach to the public-private divide, especially in the jurisprudence on the positive obligations of the UK. Unlike the law of confidentiality or data protection, no market approach played any significant role in its history. Initially, the right to private life reflected a state-restrictive approach, although elements of the individual and state-facilitative approaches were present from the beginning. There is evidence of a variety of approaches during the drafting process and a degree of compromise between, or the coexistence of, state-restrictive and individual approaches in the development of the public-private divide. The picture is more complex than mere struggle but neither is it one of a linear march towards an ever purer individual approach. Instead, the ECHR jurisprudence demonstrates parallel approaches have both strengthened over time. Of course, an individual approach would not necessarily object to robust controls on public authorities but would seek equivalent protection against private actors, which is not a general concern of state-restrictive approaches. There is therefore some scope for tensions and struggles between these approaches.

Despite a significant erosion of the public-private divide under the influence of an individual approach, a state-restrictive approach has remained present, even strengthened, in the jurisprudence of the ECtHR. The development of the public-private divide in this area does not reflect a straightforward shift from one paradigm to another. Rather, it reflects the compromises struck following tensions and struggles between advocates of individual and state-restrictive approaches and parallel developments which reflect different approaches. The chapter therefore both resists accounts of a linear paradigmatic shift and accounts that privilege struggle as a core feature of information law. This history demonstrates the

influence of several distinctive approaches to the public-private divide at the heart of the regulation of individual information through the ECHR. It demonstrates complex relationships between them.

Both the drafters of Article 8 ECHR and its judicial interpreters, the European Commission of Human Rights and the European Court of Human Rights (ECtHR), played important roles in the development of the public-private divide. This chapter first considers the approach taken by Article 8 ECHR's drafters and argues that there is greater evidence of a tension of approach, even at the earliest stage, than observed in traditional accounts.[1] Next, the chapter examines the development of positive obligations on the State to regulate private actors and argues that, although this demonstrates clear evidence of the growing importance of an individual approach, these developments also reflect enduring conceptual struggles and parallel state-restrictive tendencies, which existing explanations of these legal changes neglect.[2] Finally, the chapter presents further evidence for the continuing presence and influence of a state-restrictive approach alongside an individual approach. This is found in the continuing rhetoric of the ECtHR,[3] the ECtHR's treatment of State surveillance,[4] and the ECtHR's approach to the doctrine of imputation.[5] It is also especially apparent in a parallel trend of the ECtHR to elaborate and intensify the requirements of the negative obligation on the state for public authorities. To that extent, it identifies a resurgence of a state-restrictive approach. National law regulating public authorities must still achieve standards of precision, detail, foreseeability and accessibility, with substantive safeguards and effective controls, quite beyond those required by national law regulating private actors.[6]

ARTICLE 8 ECHR: THE DRAFTERS' APPROACH TO THE PUBLIC-PRIVATE DIVIDE

The text of Article 8 ECHR, drafted in 1950 and in force from 3rd September 1953, provides:

> (1) Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or

[1] See below, pp. 53 to 56.
[2] See below, pp. 56 to 66.
[3] See below, pp. 67 to 68.
[4] See below, pp. 68 to 69.
[5] See below, pp. 69 to 73.
[6] See below, pp. 73 to 77.

crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

On its text alone, Article 8 ECHR reflects aspects of both individual and state-restrictive approaches. Article 8(1) ECHR expresses a broad right without reference to public or private bodies, albeit that only States are bound by the ECHR as parties. On the other hand, this must be read in light of Article 8(2) ECHR, which, as drafted, reflects a clear state-restrictive approach to the public-private divide. Public authorities cannot interfere with Article 8(1) ECHR, save where the interference is both "in accordance with the law" and "necessary in a democratic society" for one of a list of specified "interests". The text is silent on its application to private actors or the limits to which private actors might need to be subject for the state to comply with Article 8(1) ECHR. The importance of a state-restrictive approach, by contrast, is clear on the face of Article 8 ECHR.

Many commentators have observed that the ECHR was first conceived as a means to prevent interference with human rights by public authorities.[7] Kilkelly characterises the ECHR as "a response to the atrocities of the Second World War."[8] Campbell argues that this historical context limited the drafters' perspective: "dictatorship and abuse of state power [were] largely in mind".[9] This characterisation of the historical context might indicate that a consensus around a state-restrictive model would be present in the drafting materials for Article 8 ECHR. However, I contend that the drafting history reveals that an individual approach was contemplated by the drafters and shaped this final text, whereas those other accounts emphasise a state-restrictive approach of early human rights to the exclusion of an individual approach. Both approaches were present at the time of drafting Article 8 ECHR and shaped that draft in ways that were significant for the development of the public-private divide.

Although Digglemann and Cleis attribute an important role to "coincidence" in the drafting process and regret the lack of explanation for the drafting decisions in the available materials,[10] some materials do point to conceptual disagreement as an explanation for the text and structure of Article 8 ECHR. Digglemann and Cleis note that, following discussions

---

[7] See Maija Pitkänen*, Fair and Balanced Positive Obligations – Do They Exist?* (2012) EHLR 538, 539; David Russell, *Supplementing the European Convention on Human Rights: Legislating for Positive Obligations* (2010) 61 Northern Ireland Legal Quarterly 281, 281 to 282; Rabinder Singh, *Using Positive Obligations in Enforcing Rights* (2008) 13 Judicial Review 94, 94.
[8] Ursula Kilkelly, *Protecting Children's Rights under the ECHR: the Role of Positive Obligations* (2010) 61 Northern Ireland Legal Quarterly 245, 247.
[9] AIL Campbell, *Positive Obligations under the ECHR: Deprivation of Liberty by Private Actors* (2006) (10) Edinburgh Law Review 399, 399.
[10] Oliver Digglemann and Maria Nicole Cleis, *How the Right to Privacy Became a Human Right* (2014) (14) Human Rights Law Review 441, 457.

about whether protection should extend beyond the acts of public authorities to private actors in Article 8(1) ECHR, the drafters agreed to mirror the approach taken in the Universal Declaration of Human Rights 1948 (UDHR).[11] Article 12 UDHR prohibited "arbitrary interference" with privacy, family, home or correspondence using general language that did not exhibit a public-private divide. This demonstrates that the nature of the public-private divide in Article 8 ECHR was at least considered by the drafters. However, it falls short of demonstrating a real tension between differing approaches. The drafting of Article 8(1) might merely reflect the desire for a level of consistency with the UDHR. Indeed, closer formulations to Article 12 UDHR were adopted in the early drafting history of Article 8 ECHR.[12] The development of Article 8(2) ECHR might therefore simply reflect the drafters' elaboration on "arbitrary" interference for the purpose of a public authority.

However, there is an important further piece of evidence. There was a failed attempt by the United Kingdom's negotiators to confine the right in Article 8(1) ECHR to a freedom from "governmental interference" in private and family life, home and correspondence.[13] This appears to be an attempt to ensure that interference by private actors would not be within the scope of Article 8(1) ECHR at all. The UK's failed amendment suggests the presence of a school of thought that would intensify the state-restrictive approach in Article 8 ECHR and remove the possibility of an individual approach to its interpretation. The UK's attempt to clarify a state-restrictive understanding of Article 8 ECHR was defeated in favour of a more ambiguous formulation that left room for the eventual development of ECHR jurisprudence according to an individual approach. There are two available explanations for this, either of which demonstrates greater conceptual disagreement than that for which the traditional account allows.

The first explanation for the UK's amendment is that there was a fear that private actors would be unduly constrained by Article 8 ECHR, either in its text or in its subsequent jurisprudential development. The UK's attempt to define Article 8 ECHR in terms of "governmental interference" could be an attempt to protect commercial private actors. This might seem unlikely considering the stance of the UK Government during the negotiations. The Labour Government of 1945 to 1951 was no defender of markets and actively opposed the protection of property rights in the ECHR.[14] It would be surprising therefore if UK

---

[11] *Ibid.*, p. 451.
[12] European Commission of Human Rights, Preparatory Work on Article 8 of the European Convention on Human Rights. Strasbourg, 9th August, 1956, DH (56) 12, A.28.696, TD 996/AEG/WM, pp. 2 to 4, 204 and 261 to 262; Doc. A. 116; Doc. A3 (2) 77; Doc. AS (1) 108, Article 2(4).
[13] Preparatory Work, p 6; Doc.CM/WP 4 (50) 14. (emphasis added). This was ultimately replaced by the wording now found in Article 8(2) ECHR: see Preparatory Work, pp. 6 and 8; Doc. CM 1 (50) 9, p. 3.
[14] Danny Nicol, The Constitutional Protection of Capitalism (2010), p. 131.

negotiators sought to protect private interests in the flow of information. However, Duranti has highlighted the influence of conservative UK politics on the drafting process, and the restrictive drafting might reflect their influence in trying to defend the liberties of private actors.[15] It is therefore unclear whether the intensification of a state-restrictive approach was motivated by market concerns or antagonism towards an individual approach to respect for private life.

Alternatively, the amendment might indicate that the UK sought clarity in favour of a state-restrictive approach in the context of discussions between negotiators which contemplated a broader scope for Article 8 ECHR. This might suggest that an individual approach was already sufficiently influential to merit the United Kingdom's proposed amendment. Further, the rejection of this amendment points to the existence of disagreement as to the preferred approach. Although the text is silent on its application to private actors, this choice left the door open to a more individual model of the public-private divide in Article 8 ECHR. It reflects a compromise of approach in light of disagreement. Tensions or struggle over the preferred approach therefore resulted in a compromise draft that left the public-private divide in Article 8(1) deliberately ambiguous. The result of this tension in drafting was important. A stronger consensus around an exclusively state-restrictive approach would have resulted in a right to freedom from governmental interference in private and family life. This might have restricted the avenues open to those who would later seek to develop Article 8 ECHR judicially in line with an individual approach. The more ambiguous text instead played an important role in the later development of positive obligations in Article 8 ECHR jurisprudence. It preserved opportunities for ECtHR judges to shape the public-private divide. Disagreement, struggle and compromise of approach was therefore present at the drafting of Article 8 ECHR.

ARTICLE 8 ECHR: THE INTERPRETERS' APPROACH TO THE PUBLIC-PRIVATE DIVIDE

POSITIVE OBLIGATIONS AND ARTICLE 8 ECHR

The development of positive obligations to "secure" respect for private life, even between private actors was a major jurisprudential development of Article 8 ECHR by the ECtHR.[16] Although negative obligations on public authorities in Article 8(2) ECHR had been applied very early in the ECHR jurisprudence and demonstrate the influence of a state-restrictive approach,[17] positive obligations are now widespread and varied in ECtHR jurisprudence

[15] Marco Duranti, The Conservative Human Rights Revolution (2017).
[16] Article 1 ECHR.
[17] See below, pp. 66 to 77.

across Convention rights.[18] They are pervasive[19] and "deeply embedded"[20] in ECtHR jurisprudence.

Mowbray, and later Pitkänen, describe the development of positive obligations in Article 8 ECHR as occurring in "many contexts" as part of a second wave of legal developments between the late 1970s and early 1990s, after a first wave of case law had interpreted express positive obligations in the ECHR.[21] Although the development of positive obligations accelerated for over 40 years,[22] Feldman observed in 1997 that the ECtHR had "not imposed on States the obligation to enact regulatory legislation" in relation to private actors at that time.[23] Those developments occurred only in the last 20 years. This correlates with Mowbray's, and later Pitkänen's, final period in the expansion of positive obligations under the full-time ECtHR after 1998, which Mowbray describes as both "imposing greater obligations"[24] and "developing the spectrum of such obligations."[25]

This has been understood by some to represent a fundamental change from a state-restrictive to an individual approach in European human rights.[26] Others argue that positive obligations are a response to the privatisation of traditional State functions, suggesting that the fundamental approach remains state-restrictive in nature.[27] However, I argue that neither of these explanations are completely satisfactory. The jurisprudence instead reveals the rise of a true individual approach, but tempered by the ongoing influence of the state-restrictive approach, which in relation to some parts of the jurisprudence has in fact intensified. This complex interaction is neither one of paradigm shift or straightforward conflict.

Some commentators present these legal developments as part of a greater shift from a state-restrictive towards an individual model of human rights. Kay argues that the ECHR "now extends beyond anything contemplated" by the state-restrictive original drafters and

---

[18] Singh (2008), p. 94; Rory O'Connell, *Realising Political Equality: the European Court of Human Rights and Positive Obligations in a Democracy* (2010) 61 Northern Ireland Legal Quarterly 263, 263: "diversity of measures"; Alastair Mowbray, The Development of Positive Obligations under the European Convention on Human Rights by the European Court of Human Rights (2004), preface: "many different forms".
[19] Dimitris Xenos, The Positive Obligations of the State under the European Court of Human Rights (2012), p. 4.
[20] Jean-Paul Costa, *The European Court of Human Rights: Consistency of its Case Law and Positive Obligations* (2008) 26 Netherlands Quarterly Human Rights 449, 454.
[21] Mowbray (2004), pp. 227 to 229; Pitkänen (2012), p. 541.
[22] Mowbray (2004), preface.
[23] David Feldman, *The Developing Scope of Article 8 of the European Convention on Human Rights* (1997) EHRLR 265, 272.
[24] Mowbray (2004), pp. 227 to 229; Pitkänen (2012), pp. 541 to 542.
[25] Mowbray (2004), p. 229.
[26] Xenos (2012), p. 207.
[27] Catherine Donnelly, *Positive Obligations and Privatisation* (2010) 61 Northern Ireland Legal Quarterly 209, pp. 211 to 212.

signatories.[28] Xenos argues that these developments flow from scholarly debates in the 1960s,[29] which formed part of a dynamic campaign,[30] in "response to human rights violations by private parties".[31] Xenos considers that, by the 1970s, a "new generation of Europeans" "brought up free from the complexes of the past" were able to move beyond a concern for negative liberty from interference by public authorities.[32] Dickson similarly attributes the development of positive obligations to a rejection of "the idea that human rights can be adequately protected if States content themselves with merely standing by and doing nothing".[33] Both Xenos and Dickson suggest that the project of the ECHR was always greater than defence against State interference.[34] This view reflects an individual approach. Xenos argues that there is a "growing recognition of human rights as freestanding constitutional imperatives"[35] that makes the ECHR a "system of active protection that aims ultimately at the prevention of human rights violations".[36] Although these are important observations and capture a significant trend, I seek to show below that the interaction between state-restrictive and individual approaches to the public-private divide was more complex in the development of this jurisprudence.

Other commentators see the development of positive obligations generally as a reaction to the changing structure of the state, motivated by a state-restrictive ambition. Donnelly has argued that positive obligations act to counter the "reductionist"[37] neo-liberal understanding of individuals inherent in the philosophy of privatisation, by which the state seeks to divest or refuse to assume responsibility in a particular sphere of activity,[38] although she acknowledges that positive obligations also contain an emphasis "on requiring the state to take responsibility for monitoring what happens in the context of private relations".[39] In her view, the development of positive obligations prevent the state avoiding its historic human rights obligations through restructuring. This is an underlying state-restrictive ambition, tied to historic state functions, rather than driven by a desire to protect rights equally across the public-private divide. By contrast, I consider below that positive obligations are broader than

---

[28] Richard Kay, *The European Convention on Human Rights and the Control of Private Law* (2005) EHRLR 466, 466.
[29] Xenos (2012), p. 19.
[30] *Ibid.*, p. 20.
[31] *Ibid.*, p. 37.
[32] *Ibid.*, p. 2.
[33] Brice Dickson, *Positive Obligations and the European Court of Human Rights* (2010) 61(3) NILQ 203, p. 204.
[34] Xenos (2012), p. 14; Dickson (2010), p. 204.
[35] Xenos (2012), p. 171.
[36] *Ibid.*, p. 207.
[37] Donnelly (2010), p. 212.
[38] *Ibid.*, pp. 211 and 212.
[39] *Ibid.*, p. 211.

this, reflecting aspects of a genuine individual approach, albeit alongside and interacting with state-restrictive tendencies.

The ECtHR played a decisive role in the development of positive obligations, elaborating Article 8 ECHR, the text of which was drafted to leave open interpretations other than state-restrictive ones. Several commentators note the role of the European Commission on Human Rights and ECtHR, referring to an "assertive jurisprudence",[40] "dynamic interpretation",[41] and "substantial creativity" on their part.[42] The earliest case law gives little indication of the motivation for this legal development. The characterisation of the ECHR as a "living instrument" to be interpreted "in the light of present-day conditions" in *Tyrer v United Kingdom*[43] provided important context for the creativity of the ECtHR. Positive obligations inherent in Article 8 ECHR were first recognised as possible in *Marckx v Belgium* in 1979.[44] In *X and Y v Netherlands* the ECtHR, for the first time, ruled that Article 8 ECHR obligations could include "the adoption of measures designed to secure respect for private life even in the sphere of relations of individuals between themselves."[45] This was justified by mere reference to *Airey v Ireland.*[46] However, the relevant passage cited from *Airey v Ireland* only makes passing reference to *Marckx v Belgium*.[47] There is therefore very little explanation for the general recognition of positive obligations to adopt measures regulating relations between private individuals from the more limited comments in the earlier cases. Additionally, none of these early cases on positive obligations and Article 8 ECHR involved information privacy,[48] although they provided a foundation for the later developments of positive obligations in the context of information privacy. Due to this sparse reasoning, it is very difficult to identify the cause of this initial shift or the extent to which a single coherent approach underpins it. However, if the ECtHR felt compelled by the text or structure of Article 8 ECHR to recognise positive obligations, we might expect some comment on the reason for that. The silence suggests that the courts supported the development of positive obligations and did not feel required to act by the text.

The jurisprudence of the European Commission of Human Rights initially did little to develop positive obligations to regulate private actors. The first time that the European Commission

---

[40] Kay (2005), p. 446.
[41] See David Feldman, Civil Liberties and Human Rights in England and Wales (2002), p. 53.
[42] Mowbray (2004), p. 222.
[43] (1979-1980) 2 EHRR 1, para. 31.
[44] (1979) 2 EHRR 330, para. 31.
[45] (1985) 8 EHRR 235, para. 23.
[46] (1979-1980) 2 EHRR 305. See Mowbray (2004), p. 129.
[47] See *Airey v Ireland* (1979-1980) 2 EHRR 305, para. 32.
[48] *Marckx v Belgium* (1979) 2 EHRR 330 and *Airey v Ireland* (1979-1980) 2 EHRR 305 concerned deficiencies in national family law; *X and Y v Netherlands* (1985) 8 EHRR 235 concerned deficiencies in national criminal law protecting children from sexual abuse.

of Human Rights grappled with positive obligations to regulate private actors, in the context of privacy, was in 1986 in *Winer v United Kingdom*.[49] The applicant complained that English law lacked a remedy for gross privacy violations by private actors. However, the European Commission of Human Rights decided that there was no failure to respect the applicant's rights as they were "not wholly unprotected". This was because a partially successful defamation action was available: the "absence of an actionable right to privacy under English law [did not show] a lack of respect for the applicant's private life and his home". Rather, how the State fulfilled its positive obligation was "largely within its discretion". This decision demonstrates the weakness of the positive obligation to secure private life against private actors in the mid-1980s.[50] It is inconsistent with a claim that the ECtHR was pursuing any significant individual approach to positive obligations at that time. It demonstrates that an individual approach was contemplated, albeit that the wide margin of appreciation accorded removed much of its force. This was not so of negative obligations, which were enforced against public authorities robustly.[51]

When next considered in the late 1990s, the jurisprudence on positive obligations suggests that an underlying individual model had become more important. However, there was no wholesale rejection of a public-private divide in favour of an individual approach to human rights by the wider court. Rival approaches therefore coexisted in tension. Some voices in the ECtHR went so far as to advocate the wholesale rejection of the public-private divide in favour of a full individual approach but were unsuccessful in leading a wholesale change of approach. This can be most clearly illustrated by the approach taken by Judge Wilberhaber in *Stjerna v Finland*, which was never adopted by the wider ECtHR. In *Stjerna v Finland*, Judge Wilberhaber doubted the coherence of the jurisprudence on positive and negative obligations. He preferred to "construe the notion of 'interference' so as to cover facts capable of breaching an obligation incumbent on the State under Article 8(1), whether negative or positive".[52] Judge Wilberhaber argued that this approach would "have the advantage of making it clear that in substance there is no negative/positive dichotomy as regards the State's obligations to ensure respect for private and family life, but a rather striking similarity between applicable principles."[53] However, as Mowbray has noted, Judge Wilberhaber's approach in *Stjerna* has never been adopted by the ECtHR, including at least one

[49] App. No. 10871/84 (10 July 1986).
[50] See also *JS v United Kingdom*, App. No. 191173/91 (3 January 1993), for a similar example in the early 1990s.
[51] See below, pp. 73 to 77.
[52] (1997) 24 EHRR 195, pp. 218 and 219.
[53] *Ibid.*, p. 220.

unanimous Grand Chamber decision over which Judge Wilberhaber later presided.[54] It does, however, demonstrate the existence of voices in the ECtHR which would dissolve the distinction in favour of a unified approach as early as 1997. The effect of doing this would be to introduce a pure individual model in which any interference, formerly negative or positive, would be subject to the requirements of Article 8(2) ECHR. The failure to adopt such reasoning indicates that the ECtHR continued to favour a state-restrictive approach to Article 8 ECHR, and therefore a public-private divide, albeit that there was a willingness to increase the protection for individuals against private actors, which reflects the influence of concerns typical of an individual approach.

Although the ECtHR did not adopt this individual approach to the regulation of private information, the influence and rise of an individual model is nevertheless apparent in the development of positive obligations. In *Earl Spencer v United Kingdom*, the applicants complained that highly sensitive personal information had been reported by news media, using long-range photography, without their consent.[55] The application was ultimately held to be inadmissible for failure to exhaust domestic remedies, as a remedy for breach of confidence was available and the applicants had neither demonstrated it insufficient nor ineffective. However, the European Commission of Human Rights refused to "exclude that the absence of an actionable remedy in relation to the publications of which the applicants complain could show a lack of respect for their private lives."[56] The regulation of media intrusion is quite different from a concern to ensure that the State cannot avoid its obligations through privatisation and other attempts to restructure. It suggests that the motivation is one based on an individual approach. It is concerned to protect individual interests, irrespective of whether the threat to those interests comes from a public or private actor. It cannot be related to a state-restrictive response to privatisation as the media does not perform a historic state function. This is all the clearer in the later development of the ECtHR's jurisprudence involving the media and private employers.

In *Von Hannover v Germany*, the ECtHR held for the first time that positive obligations in Article 8 ECHR required the State to protect individual information contained in photographs.[57] This was the first breach of Article 8 ECHR based on positive obligations in relation to individual information. The ECtHR rejected, as offering insufficient protection, the national courts' failure to grant injunctions against certain magazines on the basis that the applicant was a "figure of contemporary society" who must tolerate photography of her daily

[54] Mowbray (2004), p. 187.
[55] (1998) 25 EHRR CD105.
[56] *Ibid.*, para. 44.
[57] (2005) 40 EHRR 1.

life in public places.[58] The ECtHR held that the positive obligation to "adopt measures designed to secure respect for private life even in the sphere of relations of individuals between themselves" also "applies to the protection of a person's picture against abuse by others".[59] The ECtHR stated that the applicable principles to both positive and negative obligations were "similar" and included a "fair balance" between competing interests, in which the "State enjoys a certain margin of appreciation."[60] Although the jurisprudence contains a similarity of applicable principle between public and private actors, reflecting an individual approach, it accorded flexibility to States via the margin of appreciation. Similar flexibility was not accorded to the regulation of public authorities under the negative obligation on the State.[61] To that extent, a state-restrictive public-private divide endured and the same level of protection was not required by the ECtHR of States to fulfil their positive obligations.

The requirement proved to be relatively flexible in light of the margin of appreciation accorded to States and the low intensity of review by the ECtHR when a national court seeks to apply its principles. In particular, the jurisprudence has not required the State to subject private actors to the same level of detailed legislative regulation as the negative obligation on public authorities required.[62] It must be contrasted with the parallel tendency of the ECHR jurisprudence to intensify the requirements on public authorities to be "in accordance with the law", which results in a focus on clear and precise legislation to justify interference. Similar clarity and precision is not imposed on private actors. Certainly, a particular State may implement its positive obligations in a manner that removes the public-private divide, and this would be compliant with the ECHR, but this has not been *required* at European level. The margin of appreciation therefore creates a form of public-private divide. Other cases illustrate the toleration of flexibility in the regulation of private actors. Such flexibility results in a public-private divide as a result of the ongoing influence of the state-restrictive approach.

For example, in *Armoniene v Lithuania*, the margin of appreciation permitted "certain financial standards based on the economic situation of the State" to be taken into account when fulfilling the positive obligation to regulate private actors.[63] Such allowances are not accorded to the negative obligation on the State.[64] In principle, a cap on compensation for

---

[58] *Ibid.*, paras. 75 to 79.
[59] *Ibid.*, para. 57.
[60] *Ibid.*, para. 58.
[61] See below, pp. 73 to 77.
[62] *Ibid.*
[63] (2009) 48 EHRR 53, para. 46.
[64] See below, pp. 73 to 77.

breach of privacy was not "incompatible" with the obligation, provided it was not "such as to deprive the individual of his or her privacy and thereby empty the right of its effective content". The ECtHR went on to hold that the resulting level of protection was, in fact, inadequate.[65] Therefore, the jurisprudence permitted greater flexibility in regulating private actors than it permitted in regulating public authorities. This flexibility appears to countenance lower penalties in order to avoid overburdening market actors and therefore might reflect elements of a market approach.

At least in relation to the media cases discussed above, positive obligations only impose a low intensity review of the application of a civil action resolved in conformity with the criteria laid down by the ECtHR for a balancing exercise. Negative obligations jurisprudence does not share this low intensity review approach.[66] An individual approach, whereby interference is subject to the same level of protection irrespective of the source of the interference, is not fully realised in the jurisprudence. In *Von Hannover v Germany (No. 2)*, the ECtHR reiterated its jurisprudence on photography but developed the concept of the margin of appreciation.[67] The ECtHR emphasised that it would perform a "supervisory function", over both legislation and national judicial decisions, to review their compatibility "in light of the case as a whole" and without taking "the place of the national courts".[68] Provided that the decision was "in conformity with the criteria laid down in the [ECtHR's] case law",[69] only "strong reasons" could justify a "substitution" of the ECtHR's view for that of the national court.[70]

It might be objected that this case law on positive obligations is a misleading comparator. The cases above concern intrusion by the media. The context requires a balance to be struck between the privacy of the individual and the freedom of expression of others. Of course, in one respect this highlights an enduring element of the state-restrictive approach. Public authorities do not have their own ECHR rights, including freedom of expression, and therefore are more restricted in what they can do than private actors. However, it is possible to go beyond media cases to demonstrate that positive obligations on the State only *require* the State to adopt a more flexible standard of regulation of private actors than is *required* of public authorities.

The more flexible approach to private actors can be seen in the recent case of *Barbulescu v Romania*, especially when contrasted with the dissenting opinion of Judge Pinto De

---

[65] *Ibid.*, paras. 46 to 48.
[66] See below, pp. 73 to 77.
[67] (2012) 55 EHRR 15.
[68] *Ibid.*, para. 104.
[69] See *Couderc v France* [2016] EMLR 19 for a recent summary of those criteria.
[70] *Ibid.*, paras. 104 to 107.

Albuquerque in the first instance decision.[71] The applicant alleged that the domestic courts had failed to protect his Article 8 ECHR rights, which had been breached by a private employer's decision to terminate his employment based on monitoring a work email account. The applicant had been dismissed for breaking workplace rules which prevented work email accounts being used for personal purposes. There was no Article 10 ECHR right of the employer involved. In the first instance decision, the ECtHR treated the case as one concerning positive obligations, since the employer was a private company.[72] The ECtHR held that the "employer's monitoring was limited in scope and proportionate", because only the email account and no other stored documents or data were searched, and the public authorities had not "failed to strike a fair balance, within their margin of appreciation".[73] It was significant that "the employer acted within its disciplinary powers" to access the email account "in the belief that it had contained professional messages".[74] The content of the emails were not "decisive" in the domestic court.[75] The ECtHR held that "it is not unreasonable for an employer to want to verify that the employees are completing their professional tasks during working hours."[76]

The Grand Chamber of the ECtHR, in *Barbulescu v Romania*,[77] clarified the nature and scope of the State's positive obligations under Article 8 ECHR in the context of employment.[78] The Grand Chamber held that in *certain circumstances* those obligations required the State to set up a "legislative framework taking into account the various interests to be protected in a particular context".[79] The ECtHR took the view that the State had to be granted a "wide margin of appreciation in assessing the need to establish a legal framework governing the conditions in which an employer may regulate electronic or other communications of a non-professional nature by its employees in the workplace"[80] because no European consensus existed on the issue.[81] This was not unlimited, however, and the State required "adequate and sufficient safeguards against abuse" by employers,[82] including proportionality and procedural guarantees against arbitrariness.[83] In this it acknowledged the *legitimate interests* of the employer. The ECtHR set out a number of factors that were

[71] App No 61496/08 (12 January 2016).
[72] *Ibid.*, para. 53.
[73] *Ibid.*, paras. 60 to 63.
[74] *Ibid.*, para. 57.
[75] *Ibid.*, para. 58.
[76] *Ibid.*, para. 59.
[77] *Ibid.*
[78] *Ibid.*, para. 114.
[79] *Ibid.*, para. 115.
[80] *Ibid.*, para. 119.
[81] *Ibid.*, para. 118.
[82] *Ibid.*, para. 120.
[83] *Ibid.*, para. 121.

relevant for national authorities to consider, including employer notification regarding monitoring, the extent of monitoring and degree of intrusion, whether the employer "has provided *legitimate reasons* to justify monitoring", whether less intrusive methods were available, the consequences of monitoring and the use made by the employer of its fruits – "in particular whether the results were used to achieve the declared aim of the measure", and whether there were appropriate safeguards.[84] The Grand Chamber acknowledged that the employer had "a *legitimate interest* in ensuring that its employees are performing their professional duties adequately and with the necessary diligence",[85] although the national court had not afforded adequate protection and failed to strike a fair balance between the interests in stake in the particular case.[86]

The positive obligation undoubtedly erodes the public-private divide. As with the negative obligation on States, the ECHR requires a legislative framework with adequate and sufficient safeguards against abuse. It reflects the rise of an individual approach but it falls short of removing the state-restrictive public-private divide. The clearest public authority comparator is *Copland v United Kingdom*.[87] Both cases concerned employer monitoring of computer use. The interference in *Copland* was held to be unlawful because the public authority sixth-form college sought to rely on an implied power to monitor internet use, which was considered too vague to be "in accordance with the law".[88] Had the college been a private body, then presumably the same outcome as *Barbulescu* would have resulted. Each had a legitimate interest in monitoring. Indeed, reliance on an implied power implies that the monitoring was necessary or expedient for the performance of the public authorities functions. The majority approach to positive obligations in *Barbulescu* does not impose detailed requirements for legality on private actors, unlike those imposed on public authorities by the development of the negative obligation. A state-restrictive divide remains despite its softening under the influence of an individual approach.

Dissenting voices in *Barbulescu* demonstrate that a full individual approach was advocated by at least one justice: a degree of conflict is therefore apparent between the individual approach favoured by Judge Pinto De Albequerque and the state-restrictive elements retained by the majority. There is a complex interaction between the underlying state-restrictive approach and its softening by the parallel influence of an individual approach, which was not fully realised. The dissenting opinion of Judge Pinto De Albequerque in *Barbulescu* argued that "any interference by the employer with the employee's right to

---

[84] *Ibid*., para. 121 (emphasis added).
[85] *Ibid*., para. 127 (emphasis added).
[86] *Ibid*., para. 141.
[87] (2007) 44 EHRR 37.
[88] *Ibid.*, para. 47.

respect for private life and freedom of expression… must be justified in a democratic society by the protection of certain specific interests covered by the Convention" making reference to the right of others in both Article 8(2) and 10(2).[89] The opinion argued that a "comprehensive Internet use policy" was required in the workplace with "specific rules on the use of email, instant messaging, social networks, blogging and web surfing" and "transparent rules on how the Internet may be used, how monitoring is conducted, how data is secured, used and destroyed, and who has access to it".[90] Blanket bans and blanket monitoring were therefore impermissible in his view.[91] The opinion went into substantial detail as to the content and operation of such policies.[92] Judge Pinto De Albuquerque argued that such an approach was required to prevent "employers acting as a distrustful Big Brother",[93] concluding that a "human-rights centred approach… warrants a transparent internal regulatory framework, a consistent implementation policy and a proportionate enforcement strategy by employers".[94] For Judge Pinto De Albuquerque, ECHR rights had "horizontal effect", "directly binding" on public authorities and "indirectly binding" on private actors, for whose violations the State was responsible to prevent or remedy as "an obligation of *results*, not merely an obligation of *means*".[95] This is an illustration of the higher standards that a purer individual approach to private actors would require. It illustrates both that such voices exist in the ECHR and that the majority have not adopted a fully individual approach to the public-private divide. Struggle, influence, and compromise are instead apparent between individual and state-restrictive approaches. Although the Grand Chamber required more detail in the assessment of positive obligations, it nevertheless did not go so far as Judge Pinto De Albequerque in his earlier dissenting opinion. The ECtHR's lighter approach to private employers, and the rejection of Judge Pinto De Albuquerque's proposed collapse of the public-private divide, reflect both ongoing conceptual disagreement within the ECtHR as to the preferred approach. The more limited adoption of an individual approach to Article 8 ECHR than advocates of a widespread shift might have expected to see is also apparent.

THE VITALITY OF THE STATE-RESTRICTIVE APPROACH IN ECHR JURISPRUDENCE

ECHR jurisprudence on positive obligations has not fully removed Article 8 ECHR's state-restrictive public-private divide, although the influence of the individual approach eroded that divide. Both public authorities and private actors must, to some extent, be regulated by law

---

[89] App No 61496/08, dissenting opinion, paragraph 5.
[90] *Ibid.*, para. 10.
[91] *Ibid.*, para. 11.
[92] *Ibid.*, paras. 11 to 14.
[93] *Ibid.*, para. 15.
[94] *Ibid.*, para. 22.
[95] *Ibid.*, para. 23 (emphasis added).

to protect Article 8 ECHR rights. However, it is mistaken to characterise this as a gradual evolution of thought from a state-restrictive to an individual approach. There are several reasons to think that the state-restrictive approach is still favoured by many members of the ECtHR, even if limited concessions have been made to regulate private actors. Rather than a gradual evolution of thought or a paradigm shift, this points to the coexistence of the rise of an individual approach with a resurgent state-restrictive approach, sometimes in tension with one another. Although the individual approach has expanded Article 8 ECHR protections, the state-restrictive approach remains vibrant. This can be seen in the ECtHR's judicial rhetoric, its approach to state surveillance, its development of the doctrine of imputation, and its elaboration of the negative obligation on public authorities. Rather than waning in the wake of an advancing individual model, it points to the continuing vitality of the state-restrictive approach in ECHR jurisprudence.

JUDICIAL RHETORIC AND ARTICLE 8 ECHR

First, despite the development of positive obligations, the ECtHR maintains a public-private divide in its rhetoric. On many occasions, the ECtHR has noted that the "essential object and purpose" of Article 8 ECHR is "to protect the individual against arbitrary interference by the public authorities",[96] even if it has also more recently emphasised that the applicable principles are "similar" in relation to private actors.[97] The ECtHR therefore continues to emphasise a state-restrictive core to Article 8 ECHR. It is ambiguous about the extent of similarity between the regulation of public and private actors. This suggests that a state-restrictive approach is still considered relevant by members of the ECtHR. There is no clear evidence of agreement about the degree of similarity. This might point to the existence of disagreement. It at least demonstrates that a narrative of linear progress towards the individual approach does not capture the complexity of ECHR jurisprudence and the public-private divide. If a strong consensus existed within the ECtHR around an individual model, then one might expect the essential object and purpose to be expressed in broader terms. Perhaps it would be expressed as the protection of the substantive right under Article 8(1) ECHR or as an "obligation of results".[98] The emphasis of the original state-restrictive ambition and the negative obligation on public authorities instead points to the continuing importance of the state-restrictive approach. That the positive obligation to regulate private

[96] See *X and Y v Netherlands* (1985) 8 EHRR 235, para. 23; *Niemietz v Germany* (1993) 16 EHRR 97, para. 31; *Von Hannover v Germany* (2005) 40 EHRR 1; *Barbulescu v Romania* App No 61496/08 (12 January 2016), para. 52; *Ageyevy v Russia* App No 7075/10 (18 April 2013), para. 194.
[97] See, for example, *Von Hannover v Germany* (2005) 40 EHRR 1, paras. 57 and 58.
[98] See *Barbulescu v Romania* App No 61496/08 (12 January 2016), dissenting opinion, para. 23.

actors is secondary in the ECtHR's rhetoric might demonstrate that rather that the individual approach is itself secondary in the thought of the ECtHR.

STATE SURVEILLANCE AND ARTICLE 8 ECHR

The ECtHR has developed a distinctive response to one aspect of State surveillance. State surveillance is an interference with Article 8(1) ECHR.[99] Secret or covert surveillance can in principle be conducted by public authorities or private actors. A state-restrictive approach is apparent in this area in relation to legislation. The State is subject to greater control regarding surveillance because the ECtHR has recognised a distinctive form of legislative interference with Article 8 ECHR. The ECtHR is willing to carry out abstract legislative review of State surveillance powers. Private actors' proposed or potential surveillance is not subject to such scrutiny: only concrete acts of private surveillance are regulated by frameworks established pursuant to the positive obligations of the State.

First, the ECtHR has held that a "menace of surveillance" by the State can itself amount to an interference with Article 8 ECHR. In *Klass v Germany*, the ECtHR noted that secret surveillance powers over citizens were characteristic of "the police state".[100] It held that in "the *mere existence of the legislation itself*, there is involved, for all those to whom the legislation could be applied, a *menace of surveillance*", which constituted an interference.[101] Such menaces can only be created by the state, even if the state could thereby empower private actors. The jurisprudence therefore recognises an interference that is unique to public authorities and reflects a state-restrictive approach, by subjecting it to control.

However, there is an alternative argument that this in fact reflects a state-facilitative strand of thinking. The ECtHR has established that the review of legislation "*in abstracto*" is possible. This is "in recognition of the particular features of secret surveillance measures and the importance of ensuring effective control and supervision of them".[102] It is contrary to the ECtHR's normal practice of only reviewing concrete interferences.[103] The possibility of

---

[99] See *Klass v Germany* (1979-1980) 2 EHRR 214, para. 41; *Khan v United Kingdom* (2001) 31 EHRR 45, para. 25; *Hewitson v United Kingdom* (2003) 37 EHRR 31; *Chalkley v United Kingdom* (2003) 37 EHRR 30; *Lewis v United Kingdom* (2004) 39 EHRR 9; *Elahi v United Kingdom* (2007) 44 EHRR 30, para. 19; *Weber and Saravia v Germany* (2008) 46 EHRR SE5.

[100] (1979-1980) 2 EHRR 214, paras. 41 and 42.

[101] *Ibid.*; see also *Liberty v United Kingdom* (2009) 48 EHRR 1, para. 57. Although note the use of an uncover agent in public was held not to be an interference in *Ludi v Switzerland* (1993) 15 EHRR 173 because the expectations of a criminal must include the possibility that the person they deal with is an undercover agent: para. 40. See also *Martin v United Kingdom* (Admissibility) (2003) 37 EHRR CD91 on the applicant's curtailment of activities once aware of surveillance. Note also that a threat to intercept is similarly an interference with correspondence: *Iordachi v Moldova* (2012) 54 EHRR 5, paras. 29 to 35.

[102] *Kennedy v United Kingdom* (2011) 52 EHRR 4, paras. 119 to 120.

[103] *Ibid.*

review *in abstracto* means legislation can be reviewed and courts do not need to inquire into the concrete practices of the state. It therefore facilitates neither confirm nor deny policies. On the other hand, although the precise requirements have been refined and harmonised more recently,[104] the ECtHR has clarified that the "principal reason" for abstract legislative review of surveillance measures is to prevent their secrecy rendering State surveillance "unchallengeable" in national courts and the ECtHR.[105] The need for abstract review of potential State surveillance therefore arises from the privileged position of the state and the legal protection of secrecy that surrounds it. The jurisprudence therefore recognises the distinctiveness of the State and applies heightened legal scrutiny to legislation: a state-restrictive response. The recognition of legislative interferences and the ECtHR's willingness to engage in abstract review of legislation points to the endurance of a state-restrictive approach within the jurisprudence.

THE DOCTRINE OF IMPUTATION AND ARTICLE 8 ECHR

The ECtHR has consistently upheld a State-restrictive logic in its doctrine of imputation. Imputation addresses the circumstances in which acts or omissions will be attributed to a public authority for the purpose of Article 8(2) ECHR. If the history of Article 8 ECHR was one of the gradual evolution of thought from a state-restrictive to an individual approach, one might expect imputation to be more generously interpreted to protect individual rights irrespective of the source of interference. The history of the doctrine of imputation does not show this to be the case. Instead, the case law suggests that the state-restrictive approach is still influential in the ECtHR.

In 1984 in *A v United Kingdom*,[106] the European Commission of Human Rights resisted the argument that an interference by a private actor was an interference that fell within the scope of Article 8(2) ECHR. The complaint related to a barrister's clerk who had revealed a private address. The ECtHR held it was inadmissible *rationale personae* because the clerk was a private actor and not a public authority.[107] However, Bar Council disciplinary proceedings were admissible, as those proceedings were ultimately an exercise of judicial power through the oversight of barristers as officers of the court.[108] The European Commission of Human Rights in 1984 clearly upheld a public-private divide. The state-restrictive approach, as with

---

[104] *(*2011) 52 EHRR 4, para. 123; *Zakharov v Russia* (2016) 63 EHRR 17, paras. 170 to 179; *Szabo and Vissy v Hungary* (2016) 63 EHRR 3, paras. 34 to 36.
[105] (2011) 52 EHRR 4, para. 124.
[106] (1984) 6 EHRR CD583.
[107] *Ibid.*, para. 6.
[108] *Ibid.*, para. 3.

positive obligations at that time, was clearly dominant. The Commission would not impute the act of a private individual to the State.

The ECtHR later imputed some acts by private actors to the State, extending the doctrine of imputation. However, this legal development was not driven by an underlying individual approach. The later cases instead reinforce a state-restrictive logic. They act to prevent public authorities circumventing their negative obligations by relying on private actors. One such situation is active involvement by a public authority in an interference by a private party. In *Storck v Germany*, the ECtHR held that the police interfered with Article 8 ECHR rights by returning the applicant to private clinics where her rights were then violated.[109] In returning her by force and thereby rendering further treatment possible, the police "became actively involved in and therefore responsible for the applicant's ensuing medical treatment."[110] Another situation concerns a "crucial contribution" of a public authority to a scheme in which a private party interferes with Article 8 ECHR. In *MM v Netherlands*, a private individual recorded telephone calls to gather evidence of an alleged sexual assault, encouraged to do so and aided by the police.[111] The ECtHR held that there had been an "interference by a public authority".[112] This was because the police had made a "crucial contribution to the execution of the scheme".[113] The police had been responsible for the inception of the scheme and both the police and prosecutor were acting in the performance of their official duties by encouraging and aiding the recording.[114] Similarly, in *Van Vondel v Netherlands*, the ECtHR held that a private telephone recording "does not *per se* offend against [Article 8 ECHR], but that by its very nature this is to be distinguished from the covert monitoring and recording of communications by a private person *in the context of and for the benefit of an official inquiry* – criminal or otherwise – and with the *connivance and technical assistance of public investigation authorities*."[115] The authorities had provided the necessary equipment and on at least one occasion gave specific instructions to obtain information. The ECtHR considered that this amounted to "a crucial contribution to executing the scheme" and was unpersuaded that the informant was in control.[116] In both cases, the ECtHR reasoned that to treat the interference as one by a private actor would "be tantamount to allowing investigating authorities to evade their Convention responsibilities by the *use of private*

[109] (2006) 43 EHRR 6, paras. 91 and 146.
[110] *Ibid.*, para. 146.
[111] (2004) 39 EHRR 19.
[112] *Ibid.*, paras. 36 to 43.
[113] *Ibid.*
[114] *Ibid.*
[115] (2009) 48 EHRR 12, paras. 48 to 49 (emphasis added).
[116] *Ibid.*, para. 49.

agents".[117] Both "active involvement" and "crucial contribution" imputation reflect a state-restrictive approach. The doctrine is concerned with public authority involvement in interferences with Article 8 ECHR. The jurisprudence is intended to prevent public authorities circumventing Article 8(2) ECHR by using private actors. They reflect a fundamentally state-restrictive logic, albeit one that looks past the private actor to the public authority behind their actions.

The underlying approach in *Craxi v Italy* also implicitly affirms a State-restrictive public-private divide in the doctrine of imputation.[118] The case was one in which the ECtHR could have taken a broader approach to imputation if it had been motivated by an individual approach. Evidence concerning telephone tapping was released to the media during a criminal trial. It could not be determined whether the release was due to an error by the court or was the act of a party to the trial. This was because the parties and their lawyers were entitled to copies of the evidence from the court's registry and had in fact obtained copies.[119] The ECtHR held that Italy had failed to fulfil its positive obligation to ensure the safe custody of such transcripts and to make effective enquiry into their release.[120] Had a release of the information by the parties to the trial been imputed to the State, then the whole case could be resolved as a matter of negative obligation. Implicit in not taking this course is that the release of the evidence by the parties or their lawyers would not have been an interference by a public authority, crucially even if a public authority had provided them with the information. Instead, the ECtHR only considered positive obligations in the face of factual uncertainty as to who was responsible for the disclosure. This suggests that a narrow approach informed the question of imputation. That in turn shows the influence of a state-restrictive approach to the question of imputation. Had an individual approach had more influence we might expect a more expansive interpretation instead. Indeed, the positive obligation in question is very much one focussed on the security and investigative duties of the public authority itself, which reinforces the conclusion that the ECtHR's approach was state-restrictive.

One explanation for the ECtHR's narrow and state-restrictive approach to imputation might be that the ECtHR felt bound to reflect general international law on this point. It is necessary to address this because if the ECtHR was merely adopting the general approach in international law to imputation then this case law is of more limited value in evaluating the influences of state-restrictive or individual approaches to the public-private divide in

---

[117] (2004) 39 EHRR 19, para. 40 (emphasis added); see also (2009) 48 EHRR 12, paras. 48 to 49, which uses substantially the same wording.
[118] (2004) 38 EHRR 47.
[119] *Ibid.*, paras. 68 to 72.
[120] *Ibid.*, paras. 73 to 75.

individual information law. The ECHR notion of crucial contribution to the execution of the scheme, involving control, equipment, aid, encouragement or instructions, does indeed closely mirror the general approach to attribution to the State for the purposes of State responsibility in international law. The International Law Commission Draft Articles on State Responsibility for Internationally Wrongful Acts (DASRIWA) express the position in international law as it was at the time of the decisions in question. Attribution in international law included acts by persons who were in fact acting on the instructions of, or under the direction or control of, the State.[121] Although attribution was acknowledged to be complex and fact sensitive, it contained similar tests to imputation in ECHR jurisprudence:

> Such conduct [by a private individual] will be attributable to the State only if [the State] directed or controlled the specific operation and the conduct complained of was an integral part of that operation.[122]

The difficulty with this explanation of the doctrine of imputation is that the ECtHR did not expressly consider itself bound to reflect general international law on this point. In so far as reasons have been expressed by the ECtHR, those reasons reflect a desire to prevent public authorities circumventing their Article 8(2) ECHR duties. The desire was to make Article 8 ECHR effective against public authorities, rather than to mirror international law. One might also expect to see a clearer adoption of the language of instruction, direction and control from international law than is found in the cases if international law were so influential. I therefore conclude that the jurisprudence reflects a predominantly state-restrictive approach to the public-private divide, rather than a mere mirroring of international law by the ECtHR.

One case hints at a higher level of disagreement over the appropriate approach to the public-private divide in imputation than in other cases. In *Masden v Denmark (Admissibility)*, the ECtHR assumed that the case concerned an interference by a public authority and therefore the negative obligation under Article 8(2) ECHR.[123] However, the factual situation was more complex. In Danish industrial relations, rights normally granted by statutes in other countries were subject to collective agreements between labour market partners, with disputes determined by Courts of Arbitration. The complainant objected to random drug tests by his private employers under that scheme, after his civil challenge before the Courts of Arbitration had failed. It is not at all obvious that the absence of a remedy before the Courts of Arbitration for a drugs testing scheme agreed through a process of collective bargaining between private actors, then administered by a private employer, is an interference by a

[121] Article 8 DARSIWA.
[122] DARSIWA, pp. 47 to 48.
[123] (2003) 36 EHRR CD61, para. 33.

public authority. This might be thought to point to an individual approach underlying the case. An apparently private arrangement was subjected to Article 8(2) ECHR. The ECtHR, however, gives no explanation for its assumption. One simple explanation might be that the ECtHR made the assumption because the case could be resolved satisfactorily without recourse to argument and judgment on the proper characterisation of the interference. Indeed, the claim failed on other grounds.[124] However, if the ECtHR were motivated to expand the doctrine of imputation in line with a consensus around an individual model, this would be a surprising opportunity to miss. A related explanation might therefore be that there was sufficient disagreement over the proper approach to imputation within the ECtHR, but agreement as to the resolution of the case on other grounds, that the point was not developed in the judgment. The silence might therefore point towards a greater degree of internal disagreement and struggle over the appropriate approach, which was avoided rather than resolved.

The ECtHR's jurisprudence on imputation is therefore indicative of a largely State-restrictive approach adopted and sustained by the ECtHR, with some possible conceptual disagreement underlying the decision in *Masden v Denmark*.

Elaborating the Negative Obligation on Public Authorities

Although the development of positive obligations is evidence of the rising influence of an individual approach within the ECtHR, this must be viewed in light of a parallel trend to elaborate and intensify the requirements of the negative obligation on public authorities in Article 8 ECHR jurisprudence. The state-restrictive approach has not only remained present throughout the development of Article 8 ECHR, it has resurged. This is especially apparent in the jurisprudence on the meaning of "in accordance with the law". It is also found in the substantive safeguards required by the ECtHR to ensure that interferences are "necessary in a democratic society". The state-restrictive approach is still favoured in these cases, although interestingly some elements of a state-facilitative approach have also been adopted.

Whereas the quality of the regulation of private actors by the State pursuant to the positive obligations under Article 8 ECHR is noticeably flexible, entailing a relatively low level of review, both in relation to the media and private employers, the ECtHR has elaborated more stringent standards for the law regulating public authorities, if interferences are to be "in accordance with the law". This trend in legal development suggests that a state-restrictive

[124] *Ibid.*

model remains influential and exists in parallel with elements of an individual approach underlying the development of positive obligations.

The requirement for interferences by public authorities to be "in accordance with the law" has not merely developed as a result of the textual requirement of Article 8(2) ECHR. The ECtHR played an important role in these developments. It points to the ongoing influence of the state-restrictive approach: not merely its survival in the text of Article 8 ECHR. The ECtHR has gone beyond applying a simple definition of "in accordance with the law", that is, bare legality according to national law, in favour of a more demanding conception of the negative obligation that also considers the "quality of the law".[125] In *Silver v United Kingdom*, the European Commission of Human Rights, drawing on principles developed in *Sunday Times v United Kingdom*,[126] held that the principles applicable to conduct "prescribed by law/prévues par la loi" in Article 10 ECHR were applicable to "in accordance with the law/prévue par la loi" in Article 8 ECHR.[127] Those principles required "some basis in domestic law", which must be "adequately accessible" and "formulated with sufficient precision to enable the citizen to regulate his conduct".[128] The law had to indicate the scope of any discretion, although the Commission "recognised the impossibility of attaining absolute certainty in the framing of laws and the risk that the search for certainty may entail excessive rigidity".[129] Additionally, the Commission required "some form of safeguards" to subject interference to "effective control", although it resisted the idea that the "safeguard must be enshrined in the very text which authorised the imposition of restrictions".[130] In *Huvig v France*, the ECtHR did accept that "law" should be understood "in a substantive not formal sense" to include both "enactments of lower rank than statutes and unwritten law… as interpreted by the court".[131] However, it was "essential to have clear, detailed rules" so that "extrapolation from general legislative provisions or by analogy from rules governing other investigative measures" lacked clarity.[132] Although earlier cases required applicants to provide evidence that the relevant interference was not in accordance with law,[133] later case law changed this position to hold that the respondent State must identify the legal basis for an interference.[134] This itself could indicate an increased state-restrictive tendency.

---

[125] *MN v San Marino* (2016) 62 EHRR 19, para. 72.
[126] (1979-1980) 2 EHRR 245.
[127] (1983) 5 EHRR 347, para. 85.
[128] *Ibid.*, paras. 86 to 88.
[129] *Ibid.*, para. 88.
[130] *Ibid.*, paras. 85 to 90.
[131] (1990) 12 EHRR 528, para. 28. See also *Kruslin v France* (1990) 12 EHRR 547.
[132] (1990) 12 EHRR 528, paras. 32 to 33.
[133] *Murray v United Kingdom* (1995) 19 EHRR 193, para. 88; *Camenzind v Switzerland* (1999) 28 EHRR 458, para. 37.
[134] *Giovine v Italy* (2003) 36 EHRR 8, paras. 25 to 26.

The ECtHR held that an interference was not in accordance with the law because the law made the interference insufficiently foreseeable in *Malone v United Kingdom*.[135] The UK's reliance on common law powers, admittedly in the context of covert surveillance, was "obscure and open to differing interpretations" which failed to "indicate with reasonable clarity the scope and manner of exercise of the relevant discretion" and lacked sufficient guarantees against abuse so that it was not in accordance with the law.[136] There was some blurring of in accordance with the law and proportionality. General powers to do "anything necessary or expedient", the formula of implied statutory powers in the United Kingdom, were also held to be too vague to be in accordance with the law in the context of collecting, storing and monitoring employee internet use.[137] The ECtHR has also held that "a broad interpretation of an exception to the general rule militating against the disclosure of personal data might not offer sufficient guarantees against the risk of abuse and arbitrariness" and so violates Article 8 ECHR.[138] The ECtHR has also held that the law, or a court order conferring discretion,[139] must specify the "scope or conditions of the exercise of discretionary power"[140] For example, an unduly wide discretion to stop and search was held to be insufficiently circumscribed and to have inadequate safeguards in *Gillan and Quinton v United Kingdom*.[141] The ECtHR has held that it is "essential to have clear, detailed rules on the application of secret measures of surveillance, especially as the technology available for its use is continually becoming more sophisticated."[142] This is not merely the case in relation to surveillance. In relation to the creation and storage of data the ECHR has held that there must be a clear legal basis, not merely be drafted in general terms, which indicates the scope and conditions of the exercise of power to collect, record and store information.[143]

Finally, the interpretation of necessity in a democratic society has also resulted in some more exacting substantive safeguards in relation to covert surveillance,[144] search warrants,[145] and the interception of communications,[146] including judicial oversight and

---

[135] (1985) 7 EHRR 14.
[136] *Ibid.*, paras. 79 to 82.
[137] *Copland v United Kingdom* (2007) 44 EHRR 37, para. 47; contrast *Barbulescu v Romania* App. No. 61496/08 (12 January 2016).
[138] *LH v Latvia* (2015) EHRR 17, paras. 50 to 60.
[139] *Natoli v Italy* (2003) 37 EHRR 49, para. 44.
[140] *Herczegfalvy v Austria* (1993) 15 EHRR 437, para. 91.
[141] (2010) 50 EHRR 45, paras. 78 to 87.
[142] *Shimovolos v Russia* (2014) 58 EHRR 26, para. 68.
[143] *Amann v Switzerland* (2000) 30 EHRR 843, paras. 75 to 77.
[144] *Klass v Germany* (1979-1980) 2 EHRR 214, paras. 50 to 59. See also *Weber and Saravia v Germany* (2008) 46 EHRR SE5, para. 118; *Kennedy v United Kingdom* (2011) 52 EHRR 4, para. 169; *Lambert v France* (2000) 30 EHRR 346, paras. 34 to 40; *RE v United Kingdom* (2016) 63 EHRR 2, paras. 136 and 143; *Dragojevi v Croatia* (2016) 62 EHRR 25, paras. 95 and 102.
[145] *Funke v France* (1993) 16 EHRR 297, paras. 55 to 59. See also *A v Germany* (1983) 5 EHRR CD292; *Chappell v United Kingdom* (1990) 12 EHRR 1, paras. 59 to 66; *Niemietz v Germany* (1993)

standing, not merely limited to a civil remedy but including a review capable of annulling an impugned order.[147]

These judgments point to a more exacting standard than bare legality. The ECtHR has required the national law to achieve standards of precision, detail, foreseeability and accessibility with substantive safeguards and effective controls. These requirements of national legislation are far more exacting than those expressed in relation to positive obligations and suggest the ongoing importance of the influence of a state-restrictive model in the ECtHR.

On occasion, however, the ECtHR has shown greater flexibility in relation to public authorities, suggesting that a state-facilitative approach is sometimes adopted, especially in relation to national security. State-facilitative approaches have occasionally shaped the law, demonstrating a lack of one consistent approach within the ECtHR. For example, in *Malone v United Kingdom*, in an apparent concession to the practicalities of State surveillance, the ECtHR also noted that "foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly" but rather that the scope of discretion must be indicated.[148] In *Leander v Sweden*, the ECtHR held foreseeability requirements differ in the control of national security vetting so that "account may be taken also of instructions or administrative practices" to provide sufficient clarity about the scope of discretion.[149] The ECtHR noted that "absolute certainty" was both an impossibility and would lead to "excessive rigidity" in some contexts.[150] Foreseeability was therefore judged in light of appropriate advice,[151] provided the legal basis was sufficiently clear and detailed.[152] State-facilitative considerations have therefore very occasionally been influential alongside the state-restrictive and individual approaches. There is no indication, however, that these isolated examples are part of a greater trend but show the complex interaction of approaches in this field.

---

16 EHRR 97; *Miailhe v France* (1993) 16 EHRR 332, paras. 36 to 40; *Vereniging Radio 100 v Netherlands* (1996) 22 EHRR CD198; Camenzind v Switzerland (1999) 28 EHRR 458, paras. 44 to 47; *Ernst v Belgium* (2004) 39 EHRR 35, paras. 113 to 117; *Wieser v Austria* (2008) 46 EHRR 54; *Aleksanyan v Russia* (2011) 52 EHRR 18, paras. 215 to 218; *Tamosius v United Kingdom* (2002) 35 EHRR CD323.

[146] *Kennedy v United Kingdom* (2011) 52 EHRR 4, para. 158.

[147] *MN v San Marino* (2016) 62 EHRR 19, paras. 81 to 85. Bulk electronic communications interceptions and sharing intercepted data with other intelligence agencies is also currently the subject of litigation: *Big Brother Watch v United Kingdom* App. No. 24960/15.

[148] (1985) 7 EHRR 14, para. 66.

[149] (1987) 9 EHRR 433, paras. 50 to 56. See also *Esbester v United Kingdom* (1994) 18 EHRR CD72.

[150] *Petra v Romania* (2001) 33 EHRR 5, paras. 37 to 40.

[151] *Amann v Switzerland* (2000) 30 EHRR 843, paras. 56 to 57; *Peck v United Kingdom* (2003) 36 EHRR 41, paras. 66 to 67.

[152] *Doerga v Netherlands* (2005) 41 EHRR 4, paras. 47 to 54.

THE PUBLIC-PRIVATE DIVIDE IN ARTICLE 8 ECHR: COMPLEX INTERACTIONS BETWEEN DIFFERENT APPROACHES

State-restrictive and individual approaches to the public-private divide have been present in the thought of Article 8 ECHR from the beginning. There has not been a gradual evolution of thought over time. Rather, the history of Article 8 ECHR reveals the coexistence and influence of different approaches that go to the heart of the public-private divide in individual information law. Although there has been significant erosion of the public-private divide under the influence of the rising individual model, the state-restrictive approach has remained vibrant and influential in the thinking of the ECtHR, and indeed resurged in more recent case law. The state-facilitative approach has also occasionally played a small role. Accounts of the development of positive obligations that see the rejection of a state-restrictive approach in favour of an individual approach neglect the state-restrictive elaboration of the negative obligation on public authorities that paralleled those developments. They also neglect the continuing state-restrictive approach to judicial rhetoric, state surveillance and the doctrine of imputation. Although an individual approach was important for the development of positive obligations to regulate private actors, these obligations have never been as demanding as those imposed on public authorities and never vindicated a pure individual approach, which found some advocates on the court. The public-private divide in Article 8 ECHR does not reflect a gradual shift in paradigm. Nor does it reflect a simple struggle of different approaches. Instead it reflects a vibrant and deep coexistence and interaction of different approaches to the public-private divide.

CHAPTER 4

THE PUBLIC-PRIVATE DIVIDE AND UK HUMAN RIGHTS

INTRODUCTION

This chapter examines how the right to private life in Article 8 of the European Convention on Human Rights (ECHR) has shaped the public-private divide in national human rights law. It demonstrates the key role of national actors, especially legislative and judicial, in responding to ECHR jurisprudence and fashioning national legislation and the common law. European human rights law has acted as a catalyst and influence on the development of national law. National human rights law has not straightforwardly mirrored the public-private divide in Article 8 ECHR jurisprudence, but has engaged with it, characterised at times by divergence and parallel development in which state-restrictive, state-facilitative and individual approaches have all played a role. There was neither a simple shift from a state-restrictive towards an individual approach to the public-private divide, nor development that can be exclusively characterised in terms of struggle, but rather a set of complex interactions.

Prior to 1998, the right to private life in relation to individual information was in fact protected, to some extent, by the law of confidentiality, though it was not conceived in such terms. Where the United Kingdom was held to be in violation of Article 8 ECHR, reforms were sometimes implemented through ad hoc legislation.[1] The effect of Article 8 ECHR jurisprudence was therefore relatively limited. The Human Rights Act 1998 (HRA) marked a significant expansion in the protection afforded to many ECHR rights, and especially Article 8 ECHR. In 1998, the UK Government and Parliament played an important role in the resurgence and strengthening of a state-restrictive approach to the public-private divide. Although influenced or catalysed by European law, these developments were driven by national institutions. The HRA was mainly concerned to control public authorities and render legislation human rights compliant, within the limitations of parliamentary sovereignty. The judiciary in the UK also reflected state-restrictive attitudes to the scope of section 6 HRA, which made it unlawful for "public authorities" to violate the Convention rights protected by the Act. However, in the review of legislation the judiciary demonstrated both state-restrictive and state-facilitative tendencies, in some respects diverging from ECHR jurisprudence. In parallel, the rise of a more individual approach, in fashioning tort of misuse of private information, was driven first by the courts, reflecting Article 8 ECHR values but also the

[1] See Nick Taylor, *Policing, Privacy and Proportionality* (2003) European Human Rights Review 86, p. 91. For example, the judgment in *Malone v United Kingdom* (1985) 7 EHRR 14 led to Parliament passing the Interception of Communications Act 1985.

trajectory of national jurisprudence on breach of confidence, although the obligation on the national courts[2] to develop a damages action was later clarified by the ECtHR. ECtHR jurisprudence therefore reinforced the need for the development of such a tort. European jurisprudence was an influence and catalyst but the UK judiciary have not merely mirrored ECHR jurisprudence.[3]

The implementation of Article 8 ECHR in the United Kingdom by Government and Parliament brought about by the drafting of the HRA resulted in a broad shift in UK individual information law towards a state-restrictive approach to the public-private divide. Public authorities, in all they do, and those exercising public functions, when exercising those functions, were obliged to act compatibly with Article 8 ECHR.[4] Although that approach was broader that required under the ECHR, it reflected a state-restrictive ambition to constrain governmental power, albeit flexible as to the precise status of the body that held such governmental power. The national courts interpreted section 6 HRA in line with state-restrictive approaches, although admittedly not in the context of information privacy. Internal disagreements reflected tensions between rival conceptions of the public functions that required a state-restrictive approach. The national courts' jurisprudence on sections 3 and 4 HRA have required legislative regimes which interfere with Article 8 ECHR to adapt to ECHR concepts of "in accordance with law" and "proportionality".[5] The national jurisprudence has intensified the state-restrictive approach in the public-private divide regarding the right to respect for private life, prompted by repeated criticism from the ECtHR. However, aspects of the national implementation of the right to private life by the courts show a more state-facilitative streak, diverging from the approach in European human rights law. The damages available against public authorities under section 8 HRA for violations[6] have also been interpreted to take into account a state-facilitative understanding of the public interest, which has resulted in lower damages being awarded against public authorities for violations of Article 8 ECHR.[7]

A major erosion of the public-private divide regarding the protection of private information by the national courts was caused by the recognition and incremental development of the tort of misuse of private information although public authorities continue to be subject to the more restrictive jurisprudence outlined above. The development of this tort reflects attitudes

---

[2] In contrast to a positive obligation on the State as a whole: see *Peck v United Kingdom* (2003) 36 EHRR 1.
[3] See below, pp. 106 to 107.
[4] Human Rights Act 1998, s. 6.
[5] See below, pp. 87 to 95.
[6] Human Rights Act 1998, s. 7.
[7] See below, pp. 95 to 96.

characteristic of an individual approach.[8] Not only did the tort protect the right to private life in the context of private individuals' interference with Article 8 ECHR rights, but the national jurisprudence on vicarious liability in the context of the tort and public authority employees has gone some way to subject public authorities to more generous damages for violations of Article 8 ECHR by the wrongful disclosure of private information. In this way, an individual approach has mitigated the state-facilitative jurisprudence on section 8 HRA, at least in relation to the disclosure of private information.[9] The rise of an individual approach therefore acted to neutralise the effect of other state-facilitative jurisprudence.

State-restrictive, state-facilitative and individual approaches have all played a role in the shape of the public-private divide in national human rights law concerning individual information. Although influenced or catalysed by European law, these developments were driven by national institutions. The implementation of Article 8 ECHR at the national level did not simply replicate ECHR jurisprudence. The HRA itself was a rather late legislative intervention by the New Labour in 1998. The national courts had already started to develop remedies for misuse of private information before 1998 and arguably were not under a positive obligation to do so, as courts distinct from the state as a whole, until 2004, after major developments had already occurred.[10] National judicial actors have resisted and diverged from ECHR jurisprudence as well as implemented it.

THE HUMAN RIGHTS ACT 1998

The HRA was enacted by New Labour in 1998. It had a far-reaching effect on the implementation of Article 8 ECHR in the United Kingdom. Although the United Kingdom had sometimes responded legislatively to remedy particular violations of Article 8 ECHR following criticism from the ECtHR,[11] the HRA represented a comprehensive scheme to give effect to the ECHR at the national level. This was an important political decision by New Labour. It was not a reform forced upon the United Kingdom by European pressure. The United Kingdom had been subject to the ECtHR since 1950 and a right of individual petition to the ECtHR had existed since 1966. Comprehensive national legislation had not been required in the intervening decades. The drafting and passage of the HRA was instead driven by New Labour as part of its programme of national constitutional reform. The HRA's purpose was to "give further effect to rights and freedoms guaranteed under the European

[8] See below, pp. 96 to 99.
[9] See below, pp. 108 to 109.
[10] See below, p. 107.
[11] Such as the Interception of Communications Act 1985, in response to *Malone v United Kingdom* (1985) 7 EHRR 14.

Convention on Human Rights".[12] It required the courts to "take into account any judgment, decision, declaration or advisory opinion of the European Court of Human Rights".[13] It also imposed an interpretative obligation on the courts to read and give effect to primary and secondary legislation in a way which is compatible with the Convention rights to which it referred, "so far as it is possible to do so",[14] with a power to make declarations of incompatibility where it was not.[15] The effect of the legislative scheme was to require the courts to weave Convention-compliant interpretations throughout statute law. As such legislation might empower or constrain both public or private actors, this reflected an individual approach to human rights, although admittedly information privacy was not its focus. In practical terms, its importance for Article 8 ECHR in the context of the right to privacy life was also the enable the review of legislation on state surveillance and police powers.[16] Its practical focus was therefore more state-restrictive in the context of the right to private life.

Section 6 HRA also importantly imposed a duty on all public authorities, including courts and tribunals,[17] and to others in so far as they were carrying out a "public function",[18] to act compatibly with Convention rights. This statutory obligation had perhaps the most far-reaching implications for the public-private divide as it imposed enforceable duties directly on public authorities to act compatibly with Convention rights, including Article 8 ECHR. This was subject to remedies and procedures in sections 7 and 8 HRA. As drafted, this key provision of the HRA reflected a state-restrictive approach. The HRA had clear remedies for breach of section 6 on its face, whereas a remedy against private actors had to be later developed by the courts.[19]

However, this state-restrictive approach was not a mere mirror of ECHR jurisprudence. The HRA did not merely reflect the ECHR concept of a public authority.[20] As Williams notes, in Strasbourg jurisprudence "there is no equivalent of the kind of 'hybrid' liability" resulting from the public function test, as Strasbourg focuses on the institution which is alleged to have violated a right.[21] Although there are indications that the New Labour Government and

---

[12] Human Rights Act 1998, preamble.
[13] *Ibid.*, s. 2(a).
[14] *Ibid.*, s. 3(1).
[15] *Ibid.*, s. 4.
[16] See Taylor (2003).
[17] *Ibid.*, s.6(3)(a).
[18] *Ibid.*, ss. 6(3)(b) and 6(5).
[19] *Ibid.*, ss. 7 and 8.
[20] See *Aston Cantlow v Wallbank* [2003] UKHL 37; *YL v Birmingham City Council* [2007] UKHL 27.
[21] Alexander Williams, *Strasbourg's Public-Private Divide and the British Bill of Rights* [2015] EHRLR 617, 624. See also Alexander Williams, *A Fresh Perspective on Hybrid Public Authorities Under the*

Parliament intended a wider definition than that used in ECHR jurisprudence, this does not reveal an individual approach to Convention rights. Instead, it reflects a state-restrictive ambition to prevent the circumvention of the Act through privatisation and contracting out. It is therefore state-restrictive, albeit that the "state" is cast in wider terms which captured some private actors. In 1997, the Government described its definition of "public authority" as being "in wide terms", which included those "companies responsible for areas of activity which were previously within the public sector".[22] It therefore intended a wider direct application of human rights than the range of bodies that would be treated as public authorities under Strasbourg jurisprudence. Palmer argues that section 6 HRA was an attempt to "address… the reality of modern government and the increased delegation of public power to private entities".[23] This is certainly apparent from the comments by the Home Secretary Jack Straw MP in Parliament. He reflected on "the fact that many bodies, especially over the past 20 years, have performed public functions which are private, partly as a result of privatisation and partly as a result of contracting out".[24] The wording of section 6(3)(b) was in part a response to such concerns. The choices made by New Labour in Government and Parliament therefore reflected a general state-restrictive approach, albeit one distinctive from European jurisprudence.

THE DUTY ON PUBLIC AUTHORITIES AND FUNCTIONS TO ACT COMPATIBLY WITH ARTICLE 8 ECHR

It fell to the national courts to interpret the scope of section 6 HRA. As Williams noted, the scope of section 6(1) of the Human Rights Act 1998 is "one of the most controversial" aspects of the Act.[25] Williams argued that Strasbourg jurisprudence could not in principle "provide the answer to the public-function question" because it did not apply a public function test itself.[26] The debate over section 6 in the courts has shown a diversity of approach and illuminates ideological divides and concerns within the United Kingdom judiciary.[27] Bamforth, writing in 1999, noted that the "courts may be faced with a choice between according priority to the Convention approach or to that favoured in domestic law",[28] at the heart of which were

---

Human Rights Act 1998: Private Contractors, Rights-Stripping and 'Chameleonic' Horizontal Effect (2011) PL 139, 145. See also chapter 3 on imputation, pp. 69 to 73.

[22] Rights Brought Home: The Human Rights Bill (1997), Command Paper No. Cm 3782, para. 2.2.

[23] Stephanie Palmer, *Public Functions and Private Services: A Gap in Human Rights Protection* (2008) 6 International Journal of Constitutional Law 585, p. 588.

[24] H.C. Deb. 17 June 1998, vol. 314, cols. 409 to 410.

[25] Williams [2015], p. 618.

[26] *Ibid.*, p. 624.

[27] Stephanie Palmer, *Public, Private and the Human Rights Act 1998: An Ideological Divide* (2007) CLJ 559.

[28] Nicholas Bamforth, *The Application of the Human Rights Act 1998 to Public Authorities and Private Bodies* (1999) CLJ 159, pp. 162 to 163.

normative issues concerning the nature of human rights and the role of the state.[29] Although such jurisprudence was not developed exclusively in the context of cases considering individual information and Article 8 ECHR, it is nevertheless important to consider that jurisprudence here. That is because of the importance of the scope of section 6 as the key state-restrictive provision of the HRA. Even if the approach adopted by the national courts was not adopted in the context of individual information, it nevertheless shaped the public-private divide in individual information law and the general approach adopted reinforces the importance of forms of state-restrictive reasoning. It is an important counterpoint to the influence exerted by an apparent individual approach in relation to the tort of misuse of private information.

The national courts therefore arguably had considerable scope to accord a wide or narrow reading to section 6 HRA. A wider approach, seeking to extend human rights coverage as far as possible within the textual constraints of section 6, might have been suggestive of an underlying individual approach.[30] However, the differences in approach found in the case law reflect conflict, not between a state-restrictive and a strained individual approach, but rather over the appropriate definition of the state and public functions. At root these various definitions reflect the different forms of a state-restrictive ambition.

Early in the jurisprudence, the national courts interpreted section 6 to prevent the circumvention of the Act by public authorities. This marks a state-restrictive approach. For example, in *London Regional Transport* v *Mayor of London*,[31] the court held that the obligation on public authorities under section 6 entailed that public authorities could "neither contract out of the Act nor use their powers to stifle the Convention rights of others".[32] Preventing the state using its power of contract to avoid its obligations was influential in according a broad reach to human rights but it is fundamentally state-restrictive. It prohibits public authorities acting in ways that undermine rights protection in the performance of their tasks. This can also be seen in *Avocet Hardware PLC v Morrison*,[33] which considered the admissibility of intercept evidence obtained by private investigators on behalf of private parties for use in civil proceedings. The Employment Appeals Tribunal emphasised the "clearly express[ed]… public nature of the approach to cases under Article 8".[34] It criticised the Employment Tribunal for assuming "to itself the wrongdoing of the [private] Respondent",

---

[29] Bamforth (1999), p. 170.
[30] See Dawn Oliver, *The Frontiers of the State: Public Authorities and Public Function Under the Human Rights Act* [2000] PL 476.
[31] [2001] EWCA Civ 1491.
[32] *Ibid.*, para. 60.
[33] EAT/0417/02/DA (17 February 2003).
[34] *Ibid.*, para. 19.

which had led it to refuse to hear evidence that had been wrongfully obtained by a private party. The court emphasised that "it is not the Tribunal which has caused this intercept or a breach of the regulatory regime" and it had "erred in its approach to Article 8".[35] Courts and tribunals were subject to section 6 in admissibility decisions, but did not have to stand in the shoes of the private actors. The court therefore maintained a distinction between interferences by public and private actors. Section 6 was limited to a state-restrictive interpretation, whereas a court motivated by an individual approach might have upheld the broader approach to admissibility.

The courts have also interpreted section 6 according to state-restrictive approaches more generally. Although the courts disagreed on the precise scope of the state-restrictive approach to be adopted, their jurisprudence does not reflect other approaches. It is therefore broadly consistent with the wider state-restrictive approach in the HRA itself. In *Aston Cantlow and Wilmcote with Billesley Parochial Church Council* v *Wallbank*,[36] the House of Lords considered the interpretation of "public authority" and "public function" in section 6 HRA. In that case, a Parochial Church Council sought to enforce a chancel repair liability. The core disagreement between the majority and minority was over different understandings of a Parochial Church Council's functions, rather than a more fundamental difference of approach to the public-private divide. Although there was disagreement as to its scope, there was agreement as to a state-restrictive approach to section 6 HRA.

The majority emphasised the state-restrictive nature of negative obligations on public authorities in the ECHR but accepted that the HRA was drafted in broader terms to account for privatisation. Lord Nicholls argued that the "broad purpose" of section 6 was to mirror the acts for which the state is answerable in Strasbourg and to make provision for national redress.[37] "Public authority" therefore referred to bodies "whose nature is governmental in a broad sense of that expression", clear examples of which were "government departments, local authorities, the police and the armed forces".[38] He observed that "possession of special powers, democratic accountability, public funding in whole or in part, an obligation to act only in the public interest, and a statutory constitution" was "behind the instinctive classification".[39] However, he also went on to explain that section 6(3)(b) was intended to extend the concept of "public authority" to address the fact that "the manner in which wide ranging governmental functions are discharged varies considerably" and "functions of a governmental nature are frequently discharged by non-governmental bodies", sometimes as a "consequence of

[35] *Ibid.*, para. 20.
[36] [2003] UKHL 37.
[37] *Ibid.*, para. 6. See also Lord Rodger, para. 160.
[38] *Ibid.*, para. 7.
[39] *Ibid.*

privatisation".[40] He noted that "in a modern developed state governmental functions extend far beyond maintenance of law and order and defence of the realm".[41] Lord Hope adopted a similar state-restrictive approach. He emphasised that "it [was] the nature of the person itself, not the functions which it may perform, that [was] determinative" of whether a body was a public authority.[42] "Functions of a public nature", by contrast, made no such assumption and was both of "much wider reach" and "sensitive to the facts of each case".[43] "Public functions" were "clearly linked to the functions and powers, whether centralised or distributed, or government",[44] albeit that such powers could be held by private actors. The emphasis on the clear link to government highlights the state-restrictive nature of the approach, centrally concerned to control the state but conscious of a need to accommodate for cases where public functions had been placed in private hands. Lord Hobhouse, though differing in his definition, was similarly state-restrictive in approach. He emphasised that a Parochial Church Council "acts in the sectional not the public interest"[45] and was not therefore discharging a public function.[46] Although the rationale differed from Lord Nicholls and Lord Hope, the approach remained a state-restrictive one. It justified greater control of public authorities by reference to their lack of a private interest. This is state-restrictive reasoning, albeit different in focus from Lords Nicholls and Hope.

Lord Scott's dissent illustrates that the tension between the majority and minority was one of application of state-restrictive approaches, rather than a struggle between rival approaches to the public-private divide. He argued that the function of the Parochial Church Council was public because it was part of a "church by law established".[47] This entailed various rights and obligations that were not indicative of a private organisation. Anglicans, including the non-practising, were entitled to various services and parishioners, or any religion or none, were entitled to burial in the churchyard.[48] The Council's decisions to enforce were "a decision taken in the interests of the parishioners as a whole… not… private interests.[49] The fact of *establishment* as a *state* church was key to his reasoning. This was sufficient to link the Council to the state and reflects state-restrictive thinking.

This tension between different approaches to defining the scope of the state, while maintaining state-restrictive approaches, was also evident in the case in *YL* v *Birmingham*

---

[40] *Ibid.*, para. 9.
[41] *Ibid.*; see also Lord Rodger para. 159.
[42] *Ibid.*, para. 41.
[43] *Ibid.*
[44] *Ibid.*, para. 49.
[45] *Ibid.*, para. 86.
[46] *Ibid.*, para. 89.
[47] *Ibid.*, para. 130.
[48] *Ibid.*
[49] *Ibid.*

City Council.[50] The case concerned whether a private-owned care home caring for residents placed in the home by a local authority was performing a "public function". Palmer writes that the decision in *YL* "reflects different understandings of the operation of the Human Rights Act, the public-private distinction and, perhaps, more fundamentally, competing ideological stances."[51] Although this is true, the different understandings nevertheless do not reveal a fundamental departure from a state-restrictive approach but are rather variants within it. Lord Mance, in the majority, argued that the scope of section 6 was "linked to the scope of state responsibility in Strasbourg"[52] and section 6(3)(b) "merely elucidates" section 6(1).[53] This tightly and narrowly ties the concept of public function to public authority and therefore a state-restrictive approach. Lord Scott, this time in the majority, emphasised that the care home, was "simply carrying on its private business with a customer who happens to be a public authority" for a "commercial fee".[54] In his view, there was a "clear and fundamental difference" between a public authority and a private care home because the former's "activities are carried out pursuant to statutory duties and responsibilities imposed by public law", and "met by public funds", whereas the latter the duties were "whether contractual or tortious, duties governed by private law" funded by "charges agreed under private law contracts".[55] The commercial/governmental distinction is a state-restrictive one, albeit different to Lord Mance's conception.

By contrast, in dissent, Lord Bingham argued that section 6 was "a measure intended to give effective domestic protection to Convention rights" and it was therefore "appropriate to give a generously wide scope" to "public function".[56] This might be thought to reveal an individual ambition behind his dissent, it in fact reflected an effort to ensure that the state remained accountable for areas of historic responsibility. The notion of an "assumption of responsibility" by the state underpinned his understanding of a public function, for example by asking, among other things, what was "the role and *responsibility* of the state in relation to the subject matter in question",[57] looking to evidence that might "throw light on the nature and extent of the state's concern and of the *responsibility (if any) undertaken*",[58] and whether "as a matter of course or *as a last resort*, the state is… willing to pay".[59] This reflects a form

[50] [2007] UKHL 27.
[51] Palmer (2007), p. 559.
[52] [2007] UKHL 27, para. 87.
[53] *Ibid.*, para. 88.
[54] *Ibid.*, para. 27.
[55] *Ibid.*, para. 29.
[56] *Ibid.*, para. 4.
[57] *Ibid.*, para. 7 (emphasis added).
[58] *Ibid.*, para. 8 (emphasis added).
[59] *Ibid.*, para. 10 (emphasis added).

of state-restrictive logic, albeit wider than and in tension with the majority.[60] Lord Bingham argued that section 6(3)(b) was intended to "embrace" functions that were "formerly carried out by public authorities that were now carried out by private bodies."[61] Baroness Hale, also in dissent, similarly argued that "it was envisaged that purely private bodies which were providing services which has *previously been provided* by the state would be covered" by the HRA.[62] Public functions included "the exercise of the regulatory or coercive powers of the state"[63] but also included other factors including "whether the state has *assumed responsibility* for seeing that this task is performed".[64] Again, the conflict was between appropriate conceptions of the state, rather than a rejection of a state-restrictive approach in favour of an individual approach.

The HRA, as drafted, as interpreted by the courts, established a state-restrictive public-private divide in United Kingdom human rights law. This applied as much to Article 8 ECHR as any other Convention right. What disagreement was apparent was conceptual in nature, reflecting different state-restrictive approaches, rather than driven by differences between state-restrictive and individual approaches. Those developments were not required by the ECHR but reflect national development of the public-private divide by Government, Parliament and the national courts.

Review of Legislation for Compatibility with Article 8 ECHR

The review of national legislation for compatibility with Article 8 ECHR under the HRA demonstrates on the one hand the enhancement and strengthening of a state-restrictive approach to the public private divide by national courts, catalysed and influenced by pressure from the ECtHR, but also some aspects of a state-facilitative approach, divergent from ECHR jurisprudence and reflecting national constitutional norms. The state-restrictive approach of the ECHR to public authority interference "in accordance with the law"[65] was embraced to an extent by the national courts, leading to a resurgence and growth in state-restrictive thinking, but was also resisted in places, showing a divergent national approach. It therefore illustrates the complex interaction between approaches and between national and European levels. This runs counter to narratives of a gradual shift towards a more individual approach and a more complex dynamic than mere struggle, although struggle was a constituent part.

---

[60] *Ibid.*
[61] *Ibid.*, para. 20.
[62] *Ibid.*, para. 55 (emphasis added).
[63] *Ibid.*, para. 63.
[64] *Ibid.*, para. 66 (emphasis added).
[65] See chapter 3, pp. 73 to 77.

The HRA has had a significant impact on legislation regulating public authorities involved in crime and policing related activities. Taylor explains that the enactment of the Human Rights Act 1998, combined with repeated criticism from the ECHR over the UK's surveillance laws, made new legislation "essential".[66] He identifies the Regulation of Investigatory Powers Act 2000 as "the first comprehensive attempt" to legislate compatibly for surveillance by public authorities, including an "emphasis on necessity and proportionality".[67] Powers of search and seizure have similarly responded to the need to be proportionate.[68] Repeated criticism by the ECtHR of the UK's approach to surveillance, databases, police stop and search, and other police information gathering practices prompted the national courts to produce a national jurisprudence more exacting in terms of proportionality and the review of legislation to ensure it is "in accordance with the law".[69] The UK public-private divide therefore became more state-restrictive as a result of this prompting. It shows the resurgence of state-restrictive approaches in the UK, especially over the last 8 years, and the role of European jurisprudence in prompting that change.

In 2011, the national courts accommodated ECHR jurisprudence at odds with its previous case law, and showed a willingness to interpret legislation in a way that ensured greater proportionality. The national courts thereby implemented a more state-restrictive approach. In *R (GC)* v *Commissioner of Police of the Metropolis*,[70] the UK Supreme Court considered proportionality in the context of the indefinite retention of DNA, including retention after the acquittal of suspects. In the earlier case of *(R) Marper v Chief Constable of South Yorkshire Police*, the House of Lords had held that such retention was a justified and proportionate interference with Article 8(1) ECHR.[71] In *R (GC)*,the Supreme Court held that indefinite retention was a breach of Article 8(1) ECHR, in response to the decision of the ECtHR in *S and Marper v United Kingdom*.[72] As the relevant legislation could be read in a manner that was compatible with Article 8 ECHR, the court did so under section 3 HRA. The claimants argued that section 64(1A) of the Police and Criminal Evidence Act 1984 could not be read compatibly with the decision in *Marper*. This was because it required indefinite retention save in exceptional cases.[73] The Supreme Court disagreed. Lord Dyson commented that the statute was "silent as to how the statutory purposes [were] to be fulfilled" and that one could not "suppose that Parliament must have intended that this should be achieved in a

[66] Taylor (2003), p. 91.
[67] *Ibid.*, pp. 91 to 92.
[68] *Ibid.*, p. 95.
[69] See below, pp. 87 to 95.
[70] [2011] UKSC 21
[71] [2004] 1 WLR 2196.
[72] (2008) 48 EHRR 1169.
[73] [2011] UKSC 21, para. 20

disproportionate way so as to be incompatible with the ECHR".[74] Section 64(1A) could be exercised through a "proportionate scheme which gives effect to the statutory purposes and is compatible with the ECHR".[75] Lord Phillips argued that it did not follow from Parliament's lack of foresight of Article 8 ECHR's requirements or the present Government's intention to amend the legislation that "one must interpret section 64(1A) as requiring the police to exercise the power conferred by that section in a manner which infringes the requirements of the Convention".[76] Baroness Hale, pointing to the "clear intention of Parliament to legislate compatibly rather than incompatibly with the Convention rights",[77] denied that the subsequent criticism of the House of Lords by the ECtHR did not "inevitably" require the legislation to be read incompatibly but rather the "reverse".[78] Lord Kerr drew support from the flexible drafting of the provision to support the claim that section 64(1A) could be read otherwise than "to obtain a blanket, universally applied… policy".[79] Parliament had not attempted to "forecast comprehensively what those limits should be" and "must be taken to [intend to] to create a proportionate scheme which is compatible with the Convention".[80] The Supreme Court therefore read in a requirement for the scheme to be proportionate. In doing this, the Supreme Court took note of and responded to the criticism levelled at earlier judgments of the House of Lords regarding DNA retention in *Marper*.[81] European jurisprudence therefore acted to encourage and strengthen a state-restrictive approach at the national level. The Supreme Court also declared that the Association of Chief Police Officers' guidance was incompatible with Article 8 ECHR but, as Parliament was already considering new legislation, took no further action.[82] This should not be understood as a state-facilitative element in the reasoning, however, because it was driven by considerations relating to the separation of powers: the court considered that the guidance should be replaced but left the replacement to Parliament.[83]

In *R (T)* v *Chief Constable of Greater Manchester Police*,[84] the Supreme Court took further action to accommodate the resurgence of state-restrictive ECHR jurisprudence in national law. This was in response to the decision of the ECtHR in *MM v United Kingdom*, which had held that the relevant UK law was not "in accordance with the law" for the purposes of Article

---

[74] *Ibid.*, para. 26.
[75] *Ibid.*, para. 28.
[76] *Ibid.*, paras. 58 and 59.
[77] *Ibid.*, para. 70.
[78] *Ibid.*
[79] *Ibid.*, para. 86.
[80] *Ibid.*, para. 88.
[81] *Ibid.*, para. 15
[82] See *Ibid.*, Lord Dyson paras. 45 to 49; Lord Phillips para. 60; Baroness Hale para. 73; c.f. Lord Rodger dissent, para. 121.
[83] *Ibid.*, para 46.
[84] [2014] UKSC 35.

8(2) ECHR.[85] The case considered the inclusion of cautions, warnings or old minor convictions on criminal record checks under the Police Act 1997. T's conviction concerned minor dishonesty offences committed as a child, which had remained on T's criminal record check. The case demonstrates some disagreement as to the appropriate roles of concepts of proportionality and "in accordance with the law" but nevertheless held that the system under the Police Act 1997 was a violation of Article 8 ECHR. The majority readily incorporated state-restrictive ECHR jurisprudence into national law. Lord Reed, with whom the Lords Neuberger, Hale and Clarke agreed on the point,[86] held that the Police Act 1997 was not in accordance with the law. Lord Reed stated that "legislation which requires the indiscriminate disclosure by the state of personal data which it has collected and stored does not contain adequate safeguards against arbitrary interference" with Article 8 ECHR.[87] No margin of appreciation was available for legislation which is not in accordance with the law:[88]

> Whether a system provides adequate safeguards against arbitrary treatment, and is therefore "in accordance with the law" within the meaning of the Convention, is not a question of proportionality, and is therefore not a matter in relation to which the court allows national authorities a margin of appreciation.[89]

He reasoned that *MM* v *United Kingdom* had established

> that the legislation fails to meet the requirements for disclosure to constitute an interference 'in accordance with the law'" because "of the failure to draw any distinction on the basis of the nature of the offence, the disposal in the case, the time which has elapsed since the offence took place or the relevance of the data to the employment sought, and the absence of any mechanism for independent review of a decision to disclose data.[90]

Lord Reed further argued that, in any event, the disclosure of cautions "could not in any event be regarded as necessary in a democratic society".[91] The judgment therefore applied ECHR jurisprudence, with state-restrictive effect, to UK legislation.

The minority judgment, does however, show some resistance to this approach and therefore a tension within the Supreme Court as to the proper scope of a state-restrictive approach.

---

[85] The Times, 16 January 2013.
[86] *Ibid.*, para. 158.
[87] *Ibid.*, para. 113.
[88] *Ibid.*, para. 114.
[89] *Ibid.*, para. 115.
[90] *Ibid.*, para. 119.
[91] *Ibid.*, para. 121.

Lord Wilson, in dissent, argued that "it could not be seriously argued" that the 1997 Act was not in accordance with the law.[92] Lord Wilson considered that the appropriate safeguards were properly a matter of "necessity in a democratic society", for which the state had a margin of appreciation.[93] It should "not be resolved by reference to the principle of legality.[94] Lord Wilson was therefore resisted the conclusions of the ECtHR and would have diverged from ECHR jurisprudence is favour of a less restrictive, albeit still state-restrictive approach.

Later, in *Re Z (Children) (DNA Profiles: Disclosure)*,[95] the Court of Appeal similarly went further to accommodate ECHR jurisprudence on public authority interferences "in accordance with the law" into national jurisprudence. The judgment was a further application of *S and Marper v United Kingdom*, which addressed the ECtHR's criticisms of national law on the retention of biometric data.[96] The Court of Appeal held that section 22 of the Police and Criminal Evidence Act 1984 only permitted the police to retain and use biometric material for criminal law enforcement. Samples could therefore not be ordered for use in care proceedings.[97] The court developed its analysis of "in accordance with the law" and used it to construe the statute. Lord Dyson MR accepted that "the law must be as clear and certain as is practicable in all the circumstances".[98] He held that if the statute were interpreted so as to permit one class of biometric material to be used for other purposes but another class not to be, the law would treat the information in an "arbitrary" manner, because "there [was] no rational basis" for the difference in treatment.[99] Additionally, section 22 had "no rules for the exercise of the discretion of retaining and using seized material other than it may be so exercised for the purposes [of criminal law enforcement]".[100] To avoid arbitrariness, which would not be in accordance with law, he interpreted the provision as limited to this one purpose in both categories:

> section 22 contains no express or implied rules in relation to the retention and use of such material for any other purpose. If… section 22 were construed as authorising the retention and use of biometric material for such wider purposes, then in my view it would lack the clarity and precision required to

[92] *Ibid.*, para. 31
[93] *Ibid.*, paras. 37 and 38.
[94] *Ibid.*, para. 38.
[95] [2015] EWCA Civ 34.
[96] *Ibid.*, paras. 39 to 44.
[97] *Ibid.*, para. 46.
[98] *Ibid.*, para. 39.
[99] *Ibid.*, para. 40.
[100] *Ibid.*, para. 41.

> make it 'in accordance with the law'" as it would then be "unclear for what other purposes the material could be retained and use and for how long.[101]

Lord Dyson MR acknowledged that "the degree of precision and certainty demanded" was context-dependent and took into account practicability,[102] but that "an arbitrary and unjustified distinction between Part II biometric material and Part V biometric material"… "the exercise of discretion given by section 22 would be indeterminate and unclear".[103] State-restrictive ECHR jurisprudence on interferences "in accordance with the law" therefore prompted a more state-restrictive approach at the national level.

However, there is also some evidence of national resistance and divergence from this state-restrictive shift in response to ECtHR criticism. The UK Supreme Court at times softened the state-restrictive approach to "in accordance with the law" with more state-facilitative aspects of proportionality. For example, in *R (Catt)* v *Association of Chief Police Officers of England, Wales and Northern Ireland*,[104] the Supreme Court elaborated the requirements of "in accordance with the law" for the purposes of national law. The Supreme Court considered a challenge to the retention of personal information about an individual's attendance at demonstrations on a "domestic extremism" database by the National Public Order Intelligence Unit. The relevant information was the fact of attendance, data of birth, address and physical description as incidental references on the nominal records of other people of interest to the police. The database was based on common law powers to obtain and store information likely to assist police functions. The second claimant complained of the retention of a warning notice letter concerning an allegation of harassment. The judgment contains much that reflects the accommodation of ECHR state-restrictive jurisprudence on "in accordance with the law". Lord Sumption noted that at "common law the police have the power to obtain and store information for policing purposes", although this did not extend to intrusive methods.[105] It was subject to "an intensive regime of statutory and administrative regulation", principally the Data Protection Act 1998.[106] He defined "in accordance with the law" as "not limited to requiring an ascertainable legal basis for the interference as a matter of domestic law… also ensures that the law is not so wide or indefinite as to permit interference with the right on an arbitrary or abusive basis".[107] He noted earlier national

[101] *Ibid.*, para. 43.
[102] *Ibid.*, para. 42.
[103] *Ibid.*, para. 44.
[104] [2015] UKSC 9.
[105] *Ibid.*, para. 7.
[106] *Ibid.*, para. 8.
[107] *Ibid.*, para. 11.

authority before quoting the ECHR Grand Chamber in *S and Marper* v *UK* at paragraph 99, which required:

> clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness.

Lord Sumption observed that "rules need not be statutory, provided that they operate within a framework of law and that there are effective means of enforcing them" and their application is "reasonably predictable, if necessary with the assistance of expert advice", including "principles which are capable of being predictably applied to any situation".[108] The Data Protection Act 1998 "lays down principles which are germane and directly applicable to police information, and contains a framework for their enforcement on the police among others through the Information Commissioner and the courts".[109] The Police Code of Conduct provided further guidance.[110] Lord Sumption held that the domestic extremism database was "in accordance with the law".[111] This was because the relevant information was not "discreditable"[112] and was used for "proper policing purposes".[113] Information gathered for intelligence was "necessarily in the first instance indiscriminately" because "its value can only be judged in hindsight, as subsequent analysis for particular purposes discloses a relevant pattern."[114]

The judgment did however soften the state-restrictive approach in some respects. For example, it highlighted that disproportionate labour would be required to remove the references.[115] The interference was therefore "justified by the legitimate requirements of police intelligence-gathering in the interests of the maintenance of public order and the prevention of crime".[116] This is a more state-facilitative strand of thinking. ECHR jurisprudence, by contrast, requires no interference without justification. It does not take into account the resources of a public authority when determining whether interference is proportionate. By contrast, the Supreme Court took the importance of the state's functions in

---

[108] *Ibid.*
[109] *Ibid.*, para. 12.
[110] *Ibid.*, para. 13.
[111] *Ibid.*, para. 17; see also Baroness Hale, para. 47; Lord Mance, para. 57; Lord Toulson, para. 60.
[112] *Ibid.*, para. 27.
[113] *Ibid.*, para. 30.
[114] *Ibid.*, para. 31.
[115] *Ibid.*, para. 32.
[116] *Ibid.*, para. 34; see also Baroness Hale, para. 52; Lord Mance, para. 57.

relation to the maintenance of public order and the prevention of crime to justify a more generous approach to proportionality, a state-facilitative softening of approach.

Under criticism from the ECHR, the national courts have developed and applied more vigorous interpretations of proportionality and the requirement that interference be "in accordance with the law". This development marks a more state-restrictive approach in the UK to information held by public authorities, especially the police. It is an example of change occurring through pressure from the ECHR, although it also shows some evidence of an occasional state-facilitative approach and tensions within the UK Supreme Court as to how far to accommodate ECHR jurisprudence. Two further cases give additional cause to doubt how thorough this change was and suggest a level of national resistance to strict state-restrictive interpretations within the courts.

First, in *General Dental Council v Savery*,[117] concerning the dissemination of patient records within the Council without consent for the purpose of professional disciplinary proceedings,[118] the High Court held that the disclosures were in accordance with law either because the power was implied at common law or because it was implied from the 1984 Act which gave the General Dental Council its disciplinary powers.[119] This was a remarkably relaxed approach to identifying the legal ground for interfering with the Article 8 rights of the claimants. It is not clear that such broad implied powers can be "in accordance with the law" in ECHR jurisprudence.[120] The decision therefore indicates a level of judicial divergence from ECHR jurisprudence away from a state-restrictive approach.

Secondly, in *R (Ali)* v *Minister for the Cabinet Office*,[121] the High Court considered the interpretation of "in accordance with the law" for the purposes of Article 8 ECHR in the context of section 39 of the Statistics and Registration Act 2007, which permitted disclosures of census personal information for the purpose of criminal investigations. The claimants accepted that "it [was] not necessary for the interference to be prescribed in primary or secondary legislation" but rather that it could "be prescribed in guidance or statements of policy issued by the relevant public body".[122] The High Court also held that it was necessary to consider "the rules, principles and procedures in the DPA 1998… section 6 of the Human Rights Act, and… the Board's policies and operational procedures and arrangements".[123] It held that "notwithstanding the number of legal sources governing this matter, the complexity

[117] [2011] EWHC 3011 (Admin).
[118] Each additional disclosure of which was held to engage Article 8(1): *Ibid.*, para. 50.
[119] *Ibid.*, para. 45
[120] See chapter 2.
[121] [2012] EWHC 1943 (Admin).
[122] *Ibid.*, para. 18.
[123] *Ibid.*, para. 63.

of some of some of those sources, and the fact that the whole picture can only be determined by putting together the different fragments, the position is sufficiently certain to [be in accordance with the law]."[124] The High Court further observed that "it is clear that law contained in decisions of the courts can satisfy the requirement", citing *Sunday Times v UK*.[125] The court's acceptance of guidance and policy as acceptable sources to make an interference "in accordance with the law" is a surprising conclusion in light of the later ECHR jurisprudence,[126] which was significantly more demanding than *Sunday Times v United Kingdom* and which suggests a lighter touch in the decision. This might reflect divergence in line with a state-facilitative approach.

These relatively anomalous cases point to instances where the national courts might have been gentler than the full ECHR approach to "in accordance with law". However, across surveillance, stop and search and police databases, the HRA and ECHR criticism has resulted in a much more robust state-restrictive approach more generally. It does however suggest a degree of national divergence and resistance to the resurgence of a state-restrictive approach to Article 8(1) ECHR, albeit that the national courts did a great deal to accommodate it, especially in the Supreme Court, in response to ECtHR prompting.

DAMAGES AND PUBLIC AUTHORITIES

Other aspects of a more state-facilitative approach can also be identified in the decisions of the national courts. The national courts have adopted a more forgiving approach to the assessment of damages for a breach of section 6 by public authorities, albeit this was later blunted by the development of the tort of misuse of private information.[127] Damages under the Human Rights Act 1998 are calculated in light of the public interest inherent in public authority activities, reflecting a state-facilitative approach. On such an approach, the inherent value of the state's tasks justify subjecting it to reduced damages on a state-facilitative approach. The HRA requires a court to award damages only where, taking account of all the circumstances including "any other relief or remedy granted, or order made" and the :consequences of any decision", the court is "satisfied that the award is necessary to afford just satisfaction".[128] The courts have therefore held that damages are not recoverable as of right under the HRA.[129] The courts' approach to such compensation is to treat it as "of

[124] *Ibid.*, para. 64.
[125] (1979) 2 EHRR 245, para. 47. [2012] EWHC 1943 (Admin), para. 69
[126] See chapter 2.
[127] See below, pp. 95 to 96 and 108 to 109.
[128] Human Rights Act 1998, s. 8(3).
[129] *Anufrijeva v Southwark Borough Council* [2003] EWCA Civ 1406; [2004] QB 1124, para. 50.

secondary, if any, importance" to ending the infringement in question.[130] It is therefore subject to a balance between "the interests of the victim and those of the public as a whole", in which the court had a "wide discretion".[131] Damages were considered to be "a remedy of last resort" in *Anufrijeva v Southwark Borough Council*.[132] As Steele observes: "It will always be in the individual's interest to receive damages. It may or may not be in the public interest for damages to be paid."[133] The remedies available to protect individual interests against public authorities are therefore tempered by a state-facilitative approach, which is not true of private parties claiming damages for misuse of private information.[134] Lester and Pannick observe that "there is no obvious need to adopt the 'all-or-nothing' approach of tort law, whereby the individual receives either full compensation for all foreseeable and causally connected loss or no compensation at all… a lesser amount of compensation… may legitimately be taken" to reflect that full damages might not be in the public interest.[135] The result of this reasoning is ultimately state-facilitative, in so far as a claim cannot be pursued as misuse of private information, because in such cases a public authority may be subject to a damages assessment that does not fully reflect the claimants' loss. Alongside the state-restrictive approach that characterises the HRA, the courts have therefore also promoted pockets of state-facilitative reasoning which diverge from ECHR jurisprudence at the national level in relation to remedies such as damages under the HRA.

The Development of the Tort of Misuse of Private Information: The Rise of an Individual Approach

Parallel to accommodating resurgent state-restrictive ECHR jurisprudence in the context of public authority interferences with Article 8 ECHR, the national courts have also played a major role in advancing an individual approach through the development of the tort of misuse of private information. The common law did not protect privacy directly. In *Wainwright v Home Office*, the House of Lords held that the common law had no comprehensive tort of invasion of privacy.[136] The lack of remedies for breach of privacy was also noted in *Kaye v Robertson*.[137] The development of the tort of misuse of private information demonstrates the rise of individual approaches under the influence of Europe, catalysed by the HRA, but driven primarily by the national courts. The individual approach therefore runs parallel to

---

[130] *Ibid.*, para. 53.
[131] *Ibid.*, para. 56.
[132] *Ibid.*
[133] Iain Steele, *Public Law Liability - The Human Rights Act and Beyond* (2005) CLJ 8, 9.
[134] See below, pp. 109 to 110.
[135] Anthony Lester and David Pannick, *The Impact of the Human Rights Act on Private Law: The Knight's Move* (2000) 116 LQR 380, pp. 389 and 390.
[136] [2003] 3 WLR 1137.
[137] [1991] FSR 62

state-restrictive and state-facilitative developments in relation to the HRA, although it has acted to erode the public-private divide by strengthening remedies against private actors, which can in principle be brought also against public authorities, thereby undercutting section 8 HRA damages in some contexts.

First given its name by Lord Nicholls in *Campbell* v *MGN Ltd*,[138] and now a fully freestanding cause of action,[139] the tort of misuse of private information emerged out of breach of confidence. The tort had no requirement of a confidential relationship[140] and it protected the values enshrined in articles 8 and 10 ECHR.[141] In the most recent Supreme Court case of *PJS* v *News Group Newspapers*,[142] the Supreme Court confirmed that the tort of misuse of private information protected a distinctive interest from breach of confidence: protection from intrusion rather than of secrecy. In *PJS*, the claimant sought to preserve an order prohibiting News Group Newspapers from publishing private information in England and Wales, despite the widespread disclosure of that information on the internet by foreign news sources. Lord Mance, with whom Lords Neuberger, Hale and Reed agreed, explained that the tort of misuse of private information protected individuals against intrusion. It did not merely protect secrecy. This confirmed earlier authority in the lower courts. Repetition could constitute a tort of invasion of privacy.[143] This was especially so if the disclosure was through "a different medium".[144] There was a "qualitative difference in intrusiveness and distress likely to be involved in what [was] proposed by way of unrestricted publication by the English media in hard copy as well as on their own internet sites".[145] The proposed use was "would add a different and in some respects more enduring dimension to the existing invasions of privacy" so that a continuing injunction would have value.[146] The tort of misuse of private information represents an expansion of the scope of regulation for private information in the hands of private individuals and a closing of the public-private divide in national human rights law. The tort is now so well established that *PJS* v *News Group Newspapers* contained no further

---

[138] See *Campbell v MGN Ltd* [2004] 2 AC 406, para. 14, per Lord Nicholls.
[139] *Douglas v Hello! (No 3)* [2008] 1 AC 1, para. 255, per Lord Nicholls; *Vidal-Hall v Google Inc* [2015] 3 WLR 409, para. 21, per Lord Dyson MR and Sharp LJ.
[140] *Campbell v MGN Ltd* [2004] 2 AC 406, paras. 14 and 44, per Lord Nicholls and Lord Hoffmann respectively.
[141] See *Ibid.*, para. 17, per Lord Nicholls; *Murray v Express Newspapers plc* [2009] Ch 481, para. 24, per Sir Anthony Clarke MR; *McKennitt v Ash* [2006] EWCA Civ 1714, para. 11, per Buxton LJ.
[142] [2016] UKSC 26.
[143] *CTB v News Group Newspapers Ltd* [2011] EWHC 1326 (QB) and 1334 (QB), para. 32.
[144] *Ibid.*
[145] *Ibid.*, para. 35.
[146] *Ibid.*, para. 45.

discussion of its historical root or basis.[147] This erosion of the public-private divide reflects an individual approach.

The courts have considered the values protected by Article 8 ECHR equally applicable to public and private bodies.[148] In *Campbell* v *MGN Ltd*,[149] the House of Lords addressed the development of the tort of misuse of private information. Lord Nicholls noted that the "protection of various aspects of privacy is a fast developing area of the law", the development of which has been "spurred" by the HRA.[150] Although the courts of equity had long protected information through breach of confidence, Lord Nicholls argued that the "nomenclature is misleading" because the "cause of action has now firmly shaken off the limiting constraint of the need for an initial confidential relationship".[151] However, as he observed, it had changed its nature as early as *AG v Guardian Newspapers Ltd (No 2)*.[152] He argued that the "essence of the tort was better encapsulated as misuse of private information".[153] Individual information privacy was "the value underlying this cause of action".[154] For Lord Nicholls, Article 8 and 10 ECHR jurisprudence had "prompted the courts of this country to identify more clearly the different factors involved in cases where one or another of these two interests is present".[155] Lord Nicholls considered that the "values enshrined in articles 8 and 10 [were] now part of the cause of action for breach of confidence".[156] Lord Nicholls argued that "it should now be recognised that for this purpose these values are of general application… as much applicable in disputes between individuals or between an individual and a non-governmental body… as… between individuals and a public authority".[157] Lord Nicholls limited his observations to "the *values* underlying articles 8 and 10" and did not take a view on whether the ECHR had a wider effect or whether section 6 "extends to questions of substantive law".[158] The argument was clearly individual in approach to the extent that Article 8 and Article 10 ECHR *values* were concerned. In particular, Lord Hoffmann asked "why it should be worth protecting against the state but not against a private person" and answered that there was "no logical ground for saying that a person should have less protection against a private individual than he would have against

---

[147] *PJS v NGN* [2016] UKSC 26.
[148] See also *Mosley v Express Newspapers Plc* [2008] EWHC 1777 QB, para. 126, per Eady J, referring also to Council of Europe Resolution 1165 of 1998; *Murray v Express Newspapers Plc* [2009] Ch 481, para. 24, per Sir Anthony Clarke MR.
[149] [2004] UKHL 22.
[150] *Ibid.*, para. 11.
[151] *Ibid.*, paras. 13 and 14.
[152] [1990] 1 AC 109.
[153] *Ibid.*, paras. 13 and 14.
[154] *Ibid.*, para. 15.
[155] *Ibid.*, para. 16.
[156] *Ibid.*, para. 17.
[157] *Ibid.*
[158] *Ibid.*, para. 18 (emphasis added).

the state for the publication of personal information for which there is no justification".[159] In this the driving attitude was one of an individual approach.

CATALYSED OR CAUSED BY THE HUMAN RIGHTS ACT 1998 AND ECHR?

The incremental development of the tort of misuse of private information by the national courts was catalysed by the Human Rights Act 1998 and the ECHR jurisprudence on positive obligations but it was not required or compelled by those developments, at least not initially. The rise of an individual approach in this area was not the result of a dynamic of struggle but a more cooperative and creative interaction between emerging ECHR jurisprudence and the trajectory already taken by the national courts in relation to breach of confidence.[160] More broadly, there was a lively debate surrounding the passage of the Human Rights Act concerning the extent to which the Act should have horizontal effect.[161] Over 17 years later, the Human Rights Act can be seen to have had little horizontal effect outside the development of the tort of misuse of private information. Wright observes that the absorption of ECHR principles into the common law occurred little outside the context of privacy and defamation.[162] This is one indication that the rise of an individual approach in the common law was driven by national courts. If it were driven by ECHR jurisprudence or the Human Rights Act, we might expect the absorption of ECHR principles in other contexts as well.

Several commentators argued that the development of the tort was not compelled by the HRA. For Lester and Pannick, although "the Act and the Convention rights… exert a powerful magnetic force", it was the case that "nothing in the Act prevents or inhibits the courts from developing new private law causes of action, but equally, nothing in the Act authorises the courts to do so".[163] The HRA was neutral and left development to the national courts. Quane considered that "the UK courts [were] free to extend even greater levels of protection to the Convention rights than the ECHR".[164] Bamforth argued that because the ECHR lacks a doctrine of direct effect the question "depends crucially upon the attitudes of

---

[159] *Ibid.*, para. 50.
[160] See chapter 2, pp. 31 to 33.
[161] See Basil Markesinis, *Privacy, Freedom of Expression, and the Horizontal Effect of the Human Rights Bill: Lessons from Germany* (1999) LQR 47; Murray Hunt, *The Horizontal Effect of the HRA* [1998] PL 423; Wade, *Horizons of Horizontality* (2000) 116 LQR 217, Richard Buxton, *The Human Rights Act and Private Law* (2000) 116 LQR 48; Lester and Pannick (2000); Nicholas Bamforth, *The True Horizontal Effect of the HRA 1998* (2001) LQR 34.
[162] See Jane Wright, *A Damp Squib? The Impact of Section 6 HRA on the Common Law: Horizontal Effect and Beyond* [2014] PL 289, 289.
[163] Lester and Pannick (2000), pp. 381 and 384.
[164] Helen Quane, *The Strasbourg Jurisprudence and the Meaning of a 'Public Authority' under the Human Rights Act* [2006] PL 106, 123.

national courts".[165] Buxton accepted that the debate over human rights "may act as a catalyst" in the process of developing the common law, but that it "would be a singular exercise in judicial activism".[166] For such writers, the development of the tort of misuse of private information was driven by the national courts.

Wright, by contrast, was critical of these early debates, which she argues suggested the development of horizontal effect "was a matter of judicial choice", a claim which she believes neglected "both the structure, wording and aim of the HRA itself, as well as the Strasbourg case law".[167] Hunt similarly argued in 1998 that it was irresistible that the "Human Rights Act should tend towards the horizontal end of the spectrum",[168] pointing to positive obligations in ECHR jurisprudence.[169] He argued that there was "nothing particularly novel" about the development of the common law to "achieve consistency with the Convention".[170] He also argued that section 6 precluded direct horizontal effect without requiring vertical effect because it applied the duty only to public authorities and functions.[171] However, the duty on the courts required the courts to act compatibly when developing the common law.[172] Wade argued, stronger still, that the national courts were required by the Human Rights Act to extend full horizontal effect through the "literal argument" that the obligation on the courts would act in every adjudication to require the enforcement of human rights.[173] For these writers, the national courts had little choice and were bound by broader commitments, although there was little agreement on what the effect of that would be. Such arguments would point instead to the conclusion that Europe, the UK Government and Parliament were responsible for the rise of the individual approach in UK law. I argue that the former interpretation is more convincing: the courts played a decisive role in the rise of an individual approach in individual information in this field, whereas Government and Parliament pursued a more state-restrictive approach within the Human Rights Act.

Phillipson and Williams argue persuasively that "deep constitutional norms" required the national courts to adopt an incremental approach to the development of the common law in response to section 6(3) HRA[174] and, additionally, that section 2 HRA only required Article 8

---

[165] Bamforth (2001).
[166] Buxton (2000), p. 65.
[167] Wright [2014], p. 293.
[168] Hunt [1998], p. 424.
[169] *Ibid.*, p. 437.
[170] *Ibid.*, p. 436.
[171] *Ibid.*, p. 439.
[172] *Ibid.*, p. 441.
[173] Wade (2000), pp. 217 to 218.
[174] Gavin Phillipson and Alexander Williams, *Horizontal Effect and the Constitutional Constraint* (2011) 74 MLR 878, p. 910.

ECHR to be "taken into account" as a principle or value rather than a right.[175] They argue that their "constitutional constraint model" reflects the "instinctive" approach of the national courts to the horizontal effect of the HRA.[176] Phillipson and Williams emphasised that only the State can violate Article 8 ECHR where a private actor "interferes with the interests" it protects, by failing to carry out its positive obligation to regulate the private actor.[177] The positive obligation on the State, however, does "not lead to the conclusion that the Convention rights apply horizontally"[178] but rather section 6 HRA "translated" the positive obligation of the State into the "developmental obligation of domestic courts".[179] This required incremental judicial development of the common law but not "legislative-style common law development".[180] The effect of section 6 HRA was therefore to "alter the pre-HRA position by requiring the courts to accord a greater weight to Convention principles in private common law than they previously did".[181] They argue that the HRA showed no "enacted intent" to displace the "constraint of incrementalism" on the judiciary that derives from "central features of the UK constitutional order",[182] such as democracy, the rule of law and the separation of powers.[183] Phillipson and Williams argue that Article 8 ECHR is "under-determinate",[184] an example of John Griffith's statements of "political conflict pretending to be a resolution of it".[185] Such rights were therefore "only capable of functioning in the private sphere as broad values" and not as rights, in the absence of Strasbourg jurisprudence on a particular point.[186] The HRA was therefore incapable of imposing on the national courts an "absolutely obligation" to implement Article 8 ECHR through national common law.[187]

The development of the tort of misuse of private information should be viewed in light of a broader continuity in the breach of confidence case law. Changes in breach of confidence were already occurring before 1998. Phillipson observes that the "previous stricter requirements of prior relationships of confidence and identifiable detriment had already been jettisoned" in the law of confidentiality.[188] In the 1990s, the courts were moving breach of confidence away from its basis in a relationship of confidence towards information that was

---

[175] *Ibid.*, p. 881.
[176] *Ibid.*, p. 879.
[177] *Ibid.*, p. 882.
[178] *Ibid.*, p. 883.
[179] *Ibid.*, p. 884.
[180] *Ibid.*, pp. 885 and 887.
[181] *Ibid.*, p. 886.
[182] *See also Ibid.*, p.891.
[183] *Ibid.*, pp. 887 to 888.
[184] *Ibid.*, p. 897.
[185] See John Griffith, *The Political Constitution* (1979) 42 MLR 1, 14.
[186] Phillipson and Williams (2011), p. 897.
[187] *Ibid.*, p. 897.
[188] *Ibid.*, p. 160.

confidential itself in *Attorney General v Guardian Newspapers (No 2)*.[189] This fact was viewed as highly important by the judges who developed the tort of misuse of private information, placing the development in historical continuity.[190] Lord Walker in *Douglas v Hello! (No 3)* went so far as to describe it as the "most important single step" in the development of the case law.[191] As discussed in chapter 2, the national courts were already adopting a more individual approach in relation to breach of confidence from 1968 without ECHR influence. Wright acknowledges that the decision in *Campbell* "could not plausibly be argued" to be "required by the HRA".[192] She considers that "it is arguable that the changes that have occurred… were foreshadowed long before… in [AG v Guardian Newspapers (No 2)]".[193] In *A v B plc* Lord Woolf CJ also stressed the historical origins of the tort, arguing that "the equitable origins of the action for breach of confidence" helped the court develop misuse of private information.[194] The tort was in continuity with earlier national trends drive by the national courts. In *Campbell*, Lord Nicholls similarly emphasised historical continuity in the development of the tort when he noted that the "common law or, more precisely, courts of equity have long afforded protection to the wrongful use of private information by means of the cause of action which became known as breach of confidence".[195]

The need to stress historical continuity is important. The courts have not felt free to create new causes of action,[196] as it was advocated by William Wade.[197] Baroness Hale, in *Campbell* v *MGN Ltd*, commenting on *Wainwright* v *Home Office*, emphasised that "our law cannot, even if it wanted to, develop a general tort of invasion of privacy",[198] a power that Lord Hoffmann considered previous authority was "flat against" the development of a general privacy tort as it would "distort the common law".[199] The argument and importance of historical continuity speaks to an important felt limitation on the power of the judiciary to develop the common law in an incremental fashion.[200] It also points away from a

---

[189] See *Attorney General v Guardian Newspapers (No 2)* [1990] 1 AC 109, 281, per Lord Goff.
[190] *Venables v News Group Newspapers Ltd* [2001] Fam 430, para. 31, per Dame Elizabeth Butler-Sloss P; *X v SO* [2003] EWHC QB 1101, para. 11, per Dame Elizabeth Butler-Sloss P; *Campbell v MGN Ltd* [2004] 2 AC 406, para. 14; *Campbell v MGN Ltd* [2004] 2 AC 406, paras. 47 and 85, per Lord Hoffmann and Lord Hope respectively; *Douglas v Hello! (No 3)* [2006] QB 125, para. 58, per Lord Phillips; *Douglas v Hello! (No 3)* [2008] 1 AC 1, para. 307, per Baroness Hale.
[191] *Douglas v Hello! (No 3)* [2008] 1 AC 1, para. 272, per Lord Walker.
[192] Wright [2014], p. 294.
[193] *Ibid.*
[194] *A v B plc* [2003] QB 195, para. 5, per Lord Woolf CJ.
[195] *Campbell v MGN Ltd* [2004] 2 AC 406, para. 13, per Lord Nicholls.
[196] *Venables v News Group Newspapers Ltd* [2001] Fam 430, para. 27, per Dame Elizabeth Butler-Sloss P; *Theakston v MNG Ltd* [2002] EWHC 137 QB, para. 25; *Campbell v MGN Ltd* [2004] 2 AC 406, para. 132, per Baroness Hale.
[197] Wade (2000).
[198] *Campbell v MGN Ltd* [2004] 2 AC 406, para. 133, per Baroness Hale.
[199] *Wainwright v Home Office* [2004] 2 AC 406, para. 26 and 52 respectively, per Lord Hoffmann.
[200] Phillipson and Williams, (2011).

straightforward conclusion that the Human Rights Act 1998 required the development of the tort. The courts did not say that the Human Rights Act *required* legal change. The national courts were already so acting before the HRA came into force. This helps to demonstrate that the development of the tort and its individual approach was primarily a national judicial project. Judicial understandings of the nature of the common law were both facilitator and limit. The common law was variously described by judges as continuing "to evolve, as it has done for centuries",[201] "not immutable"[202] and with the "capacity... to adapt itself to the needs of contemporary life".[203] Lord Dyson MR, in *Vidal-Hall v Google,* recognising the extent of judicial development by 2015, nevertheless commented on "the common law's perennial need (for the best of reasons, that of legal certainty) to appear not to be doing anything for the first time".[204]

Judicial development was also encouraged by reflection on the expectations of the drafters of the Human Rights Act and the low likelihood of Parliamentary legislation. Phillipson notes that the potential of the HRA to lead to a right to privacy against private actors was "one of [the Act's] most controversial aspects", which became a "primary focus of concern in Parliament".[205] The public-private divide was therefore explicitly considered during the legislative process. Lord Irvine explained in Parliament that section 6 HRA was to "apply only to public authorities… and not private individuals" because the "Convention had in its origins a desire to protect people from the misuse of power by the state".[206] The Home Secretary Jack Straw also explained that Convention rights "would not be directly justiciable in actions between private individuals".[207] However, an amendment to ensure that the courts were not treated as a "public authority" where "the parties to the proceedings before it do not include any public authority" was rejected in favour of a freedom to development the common law.[208] Lord Phillips MR in *Douglas* v *Hello! (No 3)* noted that the "Government made it clear that it does not intend to introduce legislation in relation to this area of law, but anticipates that the judges will develop the law appropriately."[209] However, Lord Phillips MR also commented that the courts did not accept the role described for them by Lord Irvine LC to develop the

---

[201] *Venables v News Group Newspapers Ltd* [2001] Fam 430, para. 80, per Dame Elizabeth Butler-Sloss P.
[202] Douglas v Hello! [2001] QB 967, p. 1011, per Keene LJ.
[203] *Campbell v MGN Ltd* [2004] 2 AC 406, para. 46, per Lord Hoffmann.
[204] *Vidal-Hall v Google Inc* [2015] 3 WLR 409, para. 19, per Lord Dyson MR and Sharp LJ.
[205] Gavin Phillipson, *The Human Rights Act, Horizontal Effect and the Common Law: A Bang or a Whimper* (1999) 62 MLR 824, p. 825.
[206] HL Deb., 3 November 1997, vol. 582, col. 1232.
[207] HC Deb., 17 June 1998, vol. 314, col. 406.
[208] See Phillipson (1999), pp. 827 and 839. HL Deb., 24 November 1997, vol. 583, cols. 771, 783 and 785. Amendment no. 32.
[209] *Douglas v Hello! (No 3)* [2006] QB 125, para. 46, per Lord Phillips.

law in line with human rights "with whole-hearted enthusiasm".[210] Although this points to greater internal disagreement within national courts, despite the trajectory of the case law, the broader point of importance is the understanding that there was an expectation, but not a requirement, of development in this area by the judiciary.

ECHR jurisprudence encouraged, but similarly did not require the courts to develop the tort of misuse of private information, at least initially. The approach of the ECHR in *Earl Spencer* v *UK* encouraged the development of the tort, as that the ECHR held in that case that Spencer had failed to exhaust his domestic remedies by failing to seek a remedy for breach of confidence.[211] This implied recognition that the common law already provided a mechanism to remedy violations of Article 8(1) ECHR was an encouragement to shape the common law. Phillipson argues that *Peck v United Kingdom*, which found that the right to an effective remedy to protect Article 8 ECHR was violated by a "lack of legal power… to award damages",[212] demonstrated that a "specific remedy" of damages was required by the ECHR and in the absence of legislative action this fell to the courts.[213]

One further cause of historical discontinuity with the common law was in fact practical. The proliferation of case law on breach of confidence, the strain placed on civil procedure for interim injunctions and the disproportionate legal costs this entailed was one factor that encouraged the courts to consolidate the law in an effort to shed the citation of historical authority in *A v B plc*.[214] This played an important role in freeing the tort of misuse of private information from historical precedent,[215] leading Lord Woolf CJ to state that "authorities which relate to the action for breach of confidence prior to the coming into force of the 1998 Act then they are largely of historic interest only."[216]

The Human Rights Act 1998 played an important role but few judges accepted that section 6(3), the duty of the courts not to act incompatibly with convention rights, required the development of the tort, at least initially. Rather there was mixed judicial comment and a wide variety of vague judicial dicta. The effect of the Human Rights Act was variously described by judges as providing "new parameters",[217] informing the prior approach,[218]

---

[210] H.L. Deb. 24 November 1997, vol. 583, col. 771., para. 46.
[211] *Venables v News Group Newspapers Ltd* [2001] Fam 430, para. 44, per Dame Elizabeth Butler-Sloss P; *Campbell v MGN Ltd* [2004] 2 AC 406, para. 48, per Lord Hoffmann; *Douglas v Hello! (No 3)* [2006] QB 125, para. 46, per Lord Phillips.
[212] (2003) 36 EHRR 41, para. 109.
[213] Gavin Phillipson, "Privacy and Breach of Confidence: The Clearest Case of Horizontal Effect?" in D Hoffmann (ed.) The Impact of the UK Human Rights Act on Private Law (2011), p. 159.
[214] *A v B plc* [2003] QB 195, paras. 7 to 10, per Lord Woolf CJ.
[215] *Ibid.*, para. 9, per Lord Woolf CJ.
[216] *Ibid.*
[217] *Ibid.*, para. 4, per Lord Woolf CJ.
[218] *Theakston v MNG Ltd* [2002] EWHC 137 QB, para. 28.

illuminating the law of breach of confidence,[219] having had an "undoubtedly.. significant influence",[220] prompting "the courts of this country to identify more clearly the different factors involved",[221] influencing "the acceptance… of the privacy of personal information as something worthy of protection in its own right",[222] and a "more subtle" development than that of the protection of Article 8 ECHR against public authorities under section 6.[223] Some doubted any greater influence could be attributed to the Human Rights Act. For example, Lord Hope in *Campbell* commented that while the "language has changed following the coming into operation of the Human Rights Act 1998 and the incorporation into domestic law of article 8 and article 10 of the Convention" he doubted whether the "centre of gravity" had really shifted what was "essentially the same" balancing exercise.[224] For some, the Human Rights Act was a "stimulus"[225] for developments, whereas for others the "1998 statute… requires these values to be acknowledged".[226] In *Mosley* v *NGN Ltd*,[227] Eady J commented that the law of confidence had been "extended in recent years under the stimulus of the Human Rights Act 1998 and the content of the Convention itself".[228] While some judgments focused on the section 6 obligation of the court,[229] Lord Hoffmann favoured the term mediation to describe the courts relationship with Article 8 ECHR:

> English law has adapted the action for breach of confidence to provide a remedy for the unauthorised disclosure of personal information… mediated by analogy to the right of privacy conferred by article 8.[230]

Much judicial commentary in the case law is by way of introduction to the real points of disagreement between the parties. Focus on the resolution of the immediate case might preclude detailed examination of the precise relationship between the common law and the Human Rights Act, especially when it did not determine the outcome between the parties. However, two points might be made. The first is that there was judicial appetite to develop the common law. We might expect a more detailed explanation of why section 6(3) required the courts to develop the common law if there were reluctance. The second is that where

---

[219] *X v SO* [2003] EWHC QB 1101, para. 13, per Dame Elizabeth Butler-Sloss P.
[220] *Campbell v MGN Ltd* [2004] 2 AC 406, para. 16, per Lord Nicholls.
[221] *Ibid.*, para. 16, per Lord Nicholls.
[222] *Ibid.*, para. 46, per Lord Hoffmann.
[223] *Ibid.*, para. 49, per Lord Hoffmann.
[224] *Ibid.*, para. 86, per Lord Hope.
[225] *Douglas v Hello! (No 3)* [2006] QB 125, para. 30, per Lord Phillips; *Mosley v News Group Newspapers Ltd* [2008] EWHC 1777 QB, para. 7, per Eady J.
[226] *Mosley v News Group Newspapers Ltd* [2008] EWHC 1777 QB, para. 7, per Eady J.
[227] [2008] EWHC 1777 (QB).
[228] *Ibid.*, para. 7.
[229] *Venables v News Group Newspapers Ltd* [2001] Fam 430, paras. 10 and 24, per Dame Elizabeth Butler-Sloss P; *A v B plc* [2003] QB 195, para. 4, per Lord Woolf CJ; *Campbell v MGN Ltd* [2004] 2 AC 406, para. 132, per Baroness Hale.
[230] *Douglas v Hello! (No 3)* [2008] 1 AC 1, para. 118, per Lord Hoffmann.

section 6(3) did impose a clearer obligation on the courts not to act in a way that was incompatible with convention rights, such as Article 10(2) negative obligations on the courts in injunction cases, the courts addressed this explicitly.[231] The way the courts addressed questions of the negative obligation under Article 10(2) stands in contrast with the reaction of the courts to any positive obligations under Article 8(1).[232] This suggests that the courts did not feel compelled by the Human Rights Act to develop the law as they did, at least initially.

The national courts have also been willing to diverge from ECHR jurisprudence. This both indicates their role in shaping the common law and lack of felt obligation to implement Article 8 ECHR jurisprudence. As Phillipson argues, the "courts do no in practice make themselves mere conduits of Strasbourg case law".[233] Phillipson points out that the national courts "appear reluctant fully to implement Strasbourg's finding in a number of decisions from *Von Hannover*"[234] and the development of the tort of misuse of private information included "a marked degree of equivocation between the values of privacy and confidentiality".[235] Phillipson doubts whether the test of a "reasonable expectation of privacy" is as broad as the information covered by Article 8 ECHR jurisprudence[236] and more broadly notes that the national courts "continue to exhibit [a] deep ambivalence towards the place and value of privacy in English law" by giving it a more narrow scope that Article 8 ECHR jurisprudence.[237] Although this does not directly address the public-private divide, it does indicate the national courts' willingness to diverge from ECHR jurisprudence. Phillipson argues that the national courts did not adopt the "extremely broad scope for Article 8" ECHR found in *Von Hannover*.[238] To that extent, the national courts' adoption of an individual approach is not as comprehensive as that found in the ECtHR's jurisprudence on positive obligations and demonstrates a degree of national divergence or resistance.

Wright argued that as the positive obligation on the state was not targeted at the national courts and could, perhaps more appropriately, have been left to Parliament, nothing in the ECHR jurisprudence required the development of the tort of misuse of private information.[239] However, the situation changed following the ECHR decision is *Von Hannover v Germany* in

---

[231] *Venables v News Group Newspapers Ltd* [2001] Fam 430, paras. 44 and 75 to 87, per Dame Elizabeth Butler-Sloss P.
[232] See *Ibid.*, paras. 25 to 27, per Dame Elizabeth Butler-Sloss P.
[233] Phillipson (2011), p. 155.
[234] Phillipson and Williams (2011), p. 906. Phillipson (2011), pp. 142 to 146.
[235] Gavin Phillipson, *Transforming Breach of Confidence – Towards a Common Law Rights of Privacy under the Human Rights Act* (2003) 66 MLR 726, p. 728.
[236] Phillipson (2011), p. 153; see also Phillipson (2003), p. 734.
[237] Phillipson (2003), p. 758. See also Gavin Phillipson, *Judicial Reasoning in Breach of Confidence Cases under the Human Rights Act: Not Taking Privacy Seriously?* (2003) EHRLR 54.
[238] Phillipson (2011), pp. 142 to 143.
[239] Wright [2014], pp. 298 to 300.

2004.[240] In *Douglas* v *Hello! (No 3),* Lord Phillips MR explained that *Von Hannover v Germany*[241] now placed an "obligation on member states to protect one individual from an unjustified invasion of private life by another individual and an *obligation on the courts of a member state* to interpret legislation in a way which will achieve that result".[242] He concluded that "so far as private information is concerned, we are required to adopt, as the vehicle for performing such duty as falls on the courts in relation to Convention rights, the cause of action formerly described as breach of confidence" to "give effect to both article 8 and 10 rights".[243] However, he was critical of this requirement: "We cannot pretend that we find it satisfactory to be required to shoehorn within the cause of action of breach of confidence claims for publication of unauthorised photographs of a private occasion".[244] Following this case the courts were more willing to suggest that the positive obligation of the State under Article 8(1) was not something that could be left to Parliament but was an obligation on the court.[245] The courts were therefore, to that extent, "required to adapt" breach of confidence to fulfil their positive obligations and therefore comply with their section 6(3) duty.[246] However, the development of the tort before 2004 suggests that national judicial development played a more significant role in the rise of the individual approach in the UK before this became the case. A stronger obligation on the national courts, rather than the United Kingdom as a whole, was a later development and cannot explain the developing jurisprudence of the courts before 2004.

THE TORT OF MISUSE OF PRIVATE INFORMATION AND PUBLIC AUTHORITIES

One further and important feature of the development of tort of misuse of private information is that it does much to undermine the state-facilitative approach to damages against public authorities under section 8 HRA. This is because the assessment of damages under the tort is generous and fully compensatory to claimants. As a tort, in principle it can be brought against public authorities either directly or, more likely, through the vicarious liability of their employees. *Axon v Ministry of Defence* suggests that the majority of employees of public authorities who are in a position to obtain private information will trigger the vicarious liability of their employer.[247] These developments undermine the earlier state-facilitative approach to section 8 damages.

---

[240] See *Douglas v Hello! (No 3)* [2006] QB 125, para. 47, per Lord Phillips.
[241] (2004) EHRR 1.
[242] *Ibid.*, paras. 47 to 49 (emphasis added).
[243] *Ibid.*, para. 53.
[244] *Ibid.*
[245] *Douglas v Hello! (No 6)* [2006] QB 125, para. 49, per Lord Phillips.
[246] See *Ibid.*
[247] [2016] EWHC 787 (QB).

Damages for the tort of misuse of private information are much more generous than section 8 HRA damages. In *Representative Claimants* v *MGN Ltd*,[248] the Court of Appeal held that damages for misuse of private information could be awarded not only for distress but also the loss or diminution of the right to control the information. The Court of Appeal adopted general principles for the award of damages, including that "certain types of information are likely to be more significant than others… [depending] on the nature of the information";[249] "the nature of the information, its significance as private information, and the effect on the victim of its disclosure" are relevant, "the effect of repeated intrusions by publication can be cumulative", and that "the extent of the damage may be claimant-specific".[250] In *Burrell* v *Clifford*,[251] the court added "the extent of the misuse"[252] to this list and suggested that the assessment "takes account of all the circumstances of the case" including "the nature of the information, the nature and extent and purpose of the misuse…, the consequences of the misuse…, whether the misuse cause the claimant financial loss or provided financial gain to the defendant, any relevant policy considerations… any mitigating factors… or aggravating factors".[253] In *J20* v *Facebook Ireland Limited*, the court considered the nature, extent and duration of the breaches and indicated that damages should "vindicate his rights and reflect the undoubted injury to his feelings".[254] The damages available under the tort of misuse of private information are therefore fully compensatory and include the vindication of the right itself. As a tort, it may be brought directly against a public authority, thereby undermining the state-facilitative approach to section 8 damages.[255] Further, the vicarious liability of employees may ground the tort and allow damages against a public authority.

In *Axon* v *Ministry of Defence*,[256] the High Court ruled on the vicarious liability of the Ministry of Defence for a tort of misuse of private information committed by an employee. The court applied the law on vicarious liability as decided by the Supreme Court in *Mohamud* v *WM Morrison Supermarkets plc*[257] and *Cox* v *Ministry of Justice*.[258] Those cases required by a relationship between the tortfeasor and the defendant and between that relationship and the tortious act.[259] An employee was straightforwardly in such a relationship.[260] Although the

[248] [2015] EWCA Civ 1291.
[249] *Ibid.*, para. 74.
[250] *Ibid,*. para. 32.
[251] [2016] EWHC 294 (QB).
[252] *Ibid.*, para. 138.
[253] *Ibid.*, para. 139.
[254] [2016] NIQB 98, para. 96.
[255] See above, pp. 95 to 96.
[256] [2016] EWHC 787 (QB).
[257] [2016] UKSC 11.
[258] [2016] UKSC 10.
[259] *Ibid.*, para. 81.
[260] *Ibid.*

employee was acting in her own interests,[261] her connection was greater than "mere opportunity"[262] because the employee worked "in a security sensitive environment", with access to Top Secret classifications, and her job included "the task to preserve that confidentiality".[263] There was "a clear and obvious connection between that wrong and that part of her job which required her to keep such information confidential".[264] The court therefore imposed vicarious liability on the Ministry of Defence.[265] It will commonly be the case that employees of public authorities work in a security sensitive environment and are tasked with preserving the confidentiality of private information in the course of their employment.[266] It will frequently be the case then that misuse of private information by civil servants or other employees of public authorities will result in vicarious liability. The effect is to reduce the public-private divide and establish more equal protection according to an individual approach. The development of the tort has therefore had another important impact on the public-private divide by undermining an earlier state-facilitative approach to damages, to the extent that the tort is available.[267]

THE PUBLIC-PRIVATE DIVIDE IN NATIONAL HUMAN RIGHTS

The decision of New Labour to pass the HRA resulted in a significant expansion of a state-restrictive approach to Article 8 ECHR in the UK. This was especially so in relation to the duties of public authorities, those carrying out public functions, and in relation to public authority surveillance, information gathering, databases and stop and search. The courts adopted a similar state-restrictive approach, both regarding the scope of section 6 and the application of concepts of proportionality and "in accordance with the law", prompted by and in response to ECtHR criticism of national jurisprudence. Despite this, some aspects of national jurisprudence show a more state-facilitative approach, including in relation to damages under the HRA. This shows national resistance and divergence from the ECHR jurisprudence and approach. The development of the tort of misuse of private information, including its generous damages provision and in light of vicarious liability, has done much to erode the public-private divide at the national level by providing remedies against private actors. An individual approach underpinned that development and was driven by the national courts, influenced and inspired but not compelled by Europe, certainly not until after the tort

[261] *Ibid.*, para. 83.
[262] *Ibid.*, para. 84.
[263] *Ibid.*, para. 92.
[264] *Ibid.*, para. 94.
[265] *Ibid.*, para. 95.
[266] See chapter 7.
[267] Some violations of Article 8 ECHR are not captured by the tort of misuse of private information. For example if the violation is due to the interference not being in accordance with law, albeit that it is otherwise proportionate.

had been substantially established. Nor was it, before 2004, clearly required by the positive obligations of the court under Article 8, given effect by section 6 HRA. Judicial development predated such developments and suggested a more cooperative role of the courts, encouraged by legislative inaction but tempered by existing attitudes towards the proper role of the courts in the UK constitution before the developing ECHR jurisprudence validated and required what was already occurring. The development of the tort of misuse of private information can be seen as in continuity with earlier case law on breach of confidence. This has undoubtedly done much to close the public-private divide and shows the role of the national courts in shaping the public-private divide in UK information law and the rise of the individual approach, including by undermining the national state-facilitative approach to damages under the HRA.

The national law on human rights therefore demonstrates a complex interaction between different approaches. Government and Parliament pursued variations on the state-restrictive approach, while national courts adopted state-restrictive approaches with some state-facilitative tendencies in their interpretation of the HRA. Those courts also contributed to a parallel development of the common law in accordance with an individual approach. This area of law demonstrates the rise of an individual approach must be understood alongside the resurgence and enhancement of a state-restrictive approach and the endurance of state-facilitative tendencies. The development is more complex than a mere struggle between different approaches. Nor does it show a straightforward shift from a state-restrictive to an individual approach to individual information law.

CHAPTER 5

THE PUBLIC-PRIVATE DIVIDE AND EUROPEAN DATA PROTECTION

INTRODUCTION

The history of the public-private divide in European data protection reflects the influence of a variety of approaches to the public-private divide: market approaches concerned to facilitate the free flow of information, individual approaches jealous to protect personal data and defend information rights against both public and private actors, state-restrictive approaches that emphasise the additional limits and legality requirements that must be placed on legitimate public authority processing; and state-facilitative approaches seeking flexibility and exemptions for public authorities in the discharge of their duties and exercise of their authority. European data protection's history gives a clear demonstration of the complex interaction of the four approaches and diverse actors in the public-private divide in individual information law. The diverse actors who shaped the public-private divide in European data protection ranged from European State governments and legislatures to networks of data protection authorities and several European and international institutions, including judicial actors. It illustrates the complexity of the projects and objectives that shaped the public-private divide.

Rather than an inevitable, inexorable shift from a state-restrictive approach and towards the individual approach, a more complex set of interactions occurred. Neither was the development of the public-private divide the result merely of struggle, although struggle undoubtedly played a role. Instead, the development of European data protection was a reaction against the state-restrictive approach in the early jurisprudence on the right to respect for private life in Article 8 ECHR. That reaction was motivated by the concerns of an individual approach. This catalysed market concerns in turn. Those market and individual concerns cooperated to drive the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data in 1981 (1981 Convention) and Data Protection Directive 46/95 EC, tempered by state-facilitative resistance from European states. European courts and latterly the European Parliament have showed more state-restrictive tendencies alongside parallel individual tendencies.

The state-restrictive approach was present in the thought of the ECJ and CJEU as it interpreted the Data Protection Directive 1995 and clearly resurged in the drafting of the GDPR. State-facilitative tendencies endured across all major legislative attempts to regulate for data protection and market approaches remained an ever present, even foundational, concern in this field. Early European data protection can only be understood as a reaction to

problems created by the deeper rejection of the state-restrictive early jurisprudence of the ECHR in favour of a more individual approach. The market approach this catalysed was concerned about the barriers to the free flow of information which were threatened by ad hoc national legislative developments across Europe.[1]

This complex picture is also found in EC and EU data protection. European data protection under the Data Protection Directive was catalysed by the individual approach favoured by a transnational network of data protection authorities but was ultimately shaped by the market approach favoured by the European Community (EC) and its institutions. At the same time, Member State governments efforts to secure state-facilitative exemptions tempered the Data Protection Directive. This was followed by a more state-restrictive model pursued by the CJEU and its predecessors under the influence of fundamental rights. The CJEU also acted ultimately to regulate private actors more robustly under the influence of fundamental rights reasoning, although this was not as comprehensive.[2] CJEU jurisprudence therefore reflects shifting or parallel state-restrictive and individual themes in its jurisprudence, similar to that found in the ECHR jurisprudence. European data protection, after the Lisbon Treaty, saw the market approach well established but transcended by individual and state-restrictive approaches driven by renewed fears about technology, globalisation and public authorities' data processing. Once again, Member States were successful in extracting many state-facilitative exemptions to key provisions as concessions.[3]

The history of the public-private divide in European data protection demonstrates the role of complex interactions between diverse approaches. It does not show any simple shift in thinking along deterministic trajectories from a state-restrictive towards an individual approach but neither does it reflect a dynamic of mere struggle. The interactions of the four approaches identified played an important role in shaping individual information law in this field.

THE EARLY DEVELOPMENT OF EUROPEAN DATA PROTECTION

In the 1970s, the Council of Europe became the first international organisation to seek to regulate data processing. This culminated in the 1981 Convention. The Council of the Organisation for Economic Cooperation and Development (OECD) similarly made recommendations in 1981 concerning guidelines governing the protection of privacy and trans-border flows of personal data. Neither of these projects sought to establish extensive rights and were drafted in abstract and general terms, with significant flexibility for national

[1] See below, pp. 114 to 119.
[2] See below, pp. 138 to 140.
[3] See below, pp. 141 to 143.

implementation and some state-facilitative exemptions, reflecting the veto power of national Governments in those negotiations. The resulting low standards and broad uniformity across the public-private divide, albeit with state-facilitative exemptions, was consistent with a market approach seeking to promote trans-border data flows.

However, to understand the rise of such projects, which reflected a market approach, albeit tempered by national state-facilitative elements, it is necessary to see them in the context of a deeper rejection of the state-restrictive approach of the ECHR by some national and sub-national European legislatures in the late 1960s and 1970s. This resulted in an uneven regulation of public and private actors across Europe. The rejection reflected a variety of attempts to secure rights consistent with an individual approach. It was this piecemeal rejection of a state-restrictive approach at the national and sub-national level, which resulted in piecemeal regulation of the private sector across Europe in particular, that generated a response from international organisations driven by a market approach. The development of European data protection was therefore the result of a complex interaction between these different approaches to the public-private divide.

Pressure from advocates of an individual approach explains the existence of market-driven responses in the first place. Indeed, without such pressure, a market approach might otherwise have simply supported an absence of regulation. The development of the public-private divide in European data protection therefore reflects a more complex interaction of approaches: neither linear progress towards the individual approach nor a mere struggle.

The development of European data protection did not occur within a core set of institutions, as in the case in the ECHR, but across national and sub-national European legislatures in response to the perceived inadequacy of ECHR jurisprudence. This produced apparently unintended consequences for European data flows and markets. The choices made by national and sub-national European legislatures thereby created a structural problem, which provided the context for the international response of the Council of Europe and the OECD. In this, preferences for individual, state-facilitative and market approaches interacted. Although the limited institutional mechanisms available, especially the prevalence of state vetoes, prevented detailed harmonisation of data protection in European markets and enabled state-facilitative exemptions to be extracted, the very existence of such responses at least points to consensus among European governments around the need for a market approach, if only at a relatively high level of abstraction and subject to state-facilitative exemptions.

REJECTION OF THE STATE-RESTRICTIVE APPROACH IN EARLY ARTICLE 8 ECHR JURISPRUDENCE

In the 1960s, privacy concerns arose alongside technological developments.[4] The "computer revolution" enabled private actors to infringe privacy in ways that were historically only available to large public authorities.[5] By the 1970s and 1980s, these fears were articulated as threats to human rights.[6] Although few actual abuses were identified,[7] policy makers feared that large private bureaucracies could use computer technology to harm individuals.[8] This encouraged an individual approach in thinking about the public-private divide in relation to personal data. Hondius considers that early government action at the national level was largely a response to such concerns.[9] Paradoxically, he observes that in many cases public authority projects were in fact the catalyst for data protection debates[10] and the "ill feeling" directed at private uses of technology manifested itself against "actual and proposed applications in the public sector."[11] Greater urgency met regulation in the public than the private sector, although a number of States introduced data protection legislation targeting private bodies as well.[12]

The development of data protection in Europe did not occur primarily within the framework of European human rights, which might seem a natural candidate for an individual approach. National legislatures instead responded to demand for regulation from the late 1960s because there was a widespread conviction, supported by contemporaneous human rights jurisprudence, that international human rights were inadequate as a means to address new technological privacy concerns.[13] First and foremost, Article 8 EHCR was at that time understood to impose only negative obligations on the state in relation to public authorities. It therefore lacked an adequate response to concerns about threats to privacy from the private sector.[14] The recognition of positive obligations to regulate private actors' use of private information did not start to develop until the late 1990s. The Committee of Experts on Human Rights made such criticisms of Article 8 ECHR in 1970.[15] A 1980 Recommendation

---

[4] See Home Department, Computers and Privacy, Cmnd 6353 (1975), para. 1. Abraham Newman, "Privacy and Regulation in a Digital Age", in Bouwman, Preissl and Steinfield (eds.), E-Life After the Dot.Com Bust (2004), p. 20.
[5] Fritz W Hondius, Emerging Data Protection in Europe (1975), p. 18.
[6] Rosemary Jay, Data Protection Law and Practice (2012), p. 1.
[7] Hondius (1975), p. 7.
[8] Hondius (1975), pp. 2 to 3.
[9] Fritz W Hondius, The Human Rights Aspect of Data Protection (1985), p. 88.
[10] *Ibid.*, p. 88.
[11] Hondius (1975), p. 4.
[12] *Ibid.*, p. 23.
[13] See, Graham Pearce and Nicholas Platten, *Achieving Personal Data Protection in the European Union* (1998) 36(4) Journal of Common Market Studies 529, 531 for commentary on this trend in the 1960s. See also Hondius (1975), p. 7.
[14] See Hondius (1975), p. 7.
[15] *Ibid.*, p. 65.

of the Parliamentary Assembly of the Council of Europe similarly considered Article 8 ECHR lacking,[16] although its proposed solution was that data protection should be added as a Protocol to the ECHR. This recommendation was supported by the European Parliament in 1982.[17]

The perceived inadequacies of Article 8 ECHR were not exclusively limited to the public-private divide. Hondius observes that the failure of Article 8 ECHR to produce the "detailed instructions" needed for effective data protection was another aspect of its inadequacy.[18] This was firstly because it was drafted in only "very general terms".[19] Furthermore, the development of ECHR jurisprudence was cumbersome and could not match "the rapid process of computerisation".[20] Finally, the ECHR was a "closed" Convention, incapable accepting members from outside Europe as the world became more global. This concern influenced the adoption of the 1981 Convention, which could address *global* information flows.[21]

The action of national legislatures produced a variety of responses, which reflected national concerns, priorities and agendas, as well as differing data protection and privacy traditions.[22] There was also very little by way of a coherent approach to data protection in the UK in the 1970s, although individual laws had some application in relation to particular privacy issues.[23] This rejection of the state-restrictive approach in Article 8 ECHR and resultant proliferation of diverse national responses generated concern for the flow of information in European markets and the barriers to trade that national legislation could create. National Governments did not, however, abandon their concern for state-facilitative approaches regarding national public authorities. This resulted in individual and market approaches increasing in influence, albeit tempered by state-facilitative concerns in early European data protection.

THE COUNCIL OF EUROPE AND PERSONAL DATA PROTECTION

In the early 1970s, the Council of Europe made calls for the harmonisation of laws on data protection. On 26 September 1973, it adopted Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector. Although the

---

[16] Recommendation 890 of 1st February 1980. See Hondius (1985), p. 90.
[17] Hondius (1985), p. 94.
[18] *Ibid.*, pp. 92 to 93.
[19] *Ibid.*, p. 90.
[20] *Ibid.*
[21] *Ibid.*, pp. 92 to 93.
[22] Hondius (1975), pp. 30 to 44.
[23] OECD Directorate for Scientific Affairs Group of Experts on Computer Utilisation, Computer Utilisation and the Privacy Problem: Summary of Replies to Questionnaire 13 April 1970 DAS/SPR/70.10, pp. 4 to 8.

Resolution was only directed at the private sector, it was understood as attempting to effect a reconciliation of the individual and market concerns. The Preamble to the Resolution recognised the need for legislation to "prevent abuses in the storing, processing and classification of personal information by means of electronic data banks in the private sector" but also stressed that it was "urgent" to "prevent further divergences between the laws of member States in this field", at least until international agreement was reached on a more extensive form of regulation. The thinking behind the Resolution was not motivated by a desire to create a public-private divide.

Further support for this can be found in the explanatory note to the Resolution, which commented that the use of computers in the public and private sectors was "not basically different."[24] The decision to prioritise the private sector in the Resolution was made by the Sub-Committee of the European Committee on Legal Co-operation in 1971, which prioritised the private sector because it was "distinctly international" and "a lack of efficient national controls might weaken the position of individuals".[25] To the extent that the earlier Resolution created a public-private divide, it was therefore one based on priority and perceived urgency rather than substance.

On 29 September 1974, the Council of Europe adopted Resolution (74) 29, which elaborated a set of principles for the public sector. The principles in the two Resolutions are substantially similar, albeit with some differences of scope. When considered together, the Resolutions reflect a market approach.

The key exception to this is the third principle of Resolution (74) 29, which sought to impose constraints on legislation permitting public authorities to carry out data processing, where processing was of "information relating to the intimate private life of individuals" or where the processing might result in unfair discrimination. Resolution (73) 22, by contrast, banned processing of such data by the private sector entirely. The third principle of Resolution (74) 29 by contrast permitted the processing of such data, subject to a requirement to make provision by law, special regulation or public statement, clearly stating the purpose of storage and use of the information and the circumstances in which it could be "communicated either within the public administration or to private persons or bodies". Such data could not be used for other purposes without explicit legal permission. To that extent, therefore, it also contained a state-restrictive element in the context of an overall more state-facilitative approach to processing data, when compared to the total ban in the private sector.

---

[24] Resolution (73) 22, explanatory note, para. 3.
[25] *Ibid.*, para. 6.

The explanatory note to the Resolution noted that it was "prudent only to formulate general principles and to leave it to the discretion of member States to decide in which fields and in what manner these principles should be implemented."[26] The Resolutions reflect a broadly market approach tempered and limited by a state-facilitative approach. This reflects the dominance of State governments and their ability to veto more extensive or detailed regulation. However, the very fact these Resolutions were passed in the early 1970s also reflects a mixture market and individual concerns. Different approaches therefore interacted, finding much common ground in the shape of the resolutions, rather than being in straightforward conflict or showing a simple rise of an individual approach. The individual approach was deeply connected to market concerns and both state-restrictive and state-facilitative elements coexisted alongside it.

THE COUNCIL OF EUROPE AND THE 1981 CONVENTION

The Council of Europe achieved a more extensive treaty with the 1981 Convention, which was opened for signature in January 1981 and signed by the United Kingdom in May 1981.[27] It was the first legally binding measure of several international attempts to harmonise data protection provisions across Europe. It shows evidence of a further attempt to reconcile individual and market considerations, and a more limited scope for potentially state-facilitative derogations.

The Preamble emphasised that it was "desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing" while "reaffirming at the same time their commitment to freedom of information regardless of frontiers" and "recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples". The 1981 Convention included public authorities within its definition of persons and bodies who were capable of being a "controller of the file".[28] It expressly provided that its scope extended to both public and private sectors.[29] Article 9 of the 1981 Convention did, however, make provision for derogations with potential application to public authorities, such as State security, public safety, the monetary interest of the State, the suppression of criminal offences, where this was provided by law and necessary in a democratic society. It sought a

[26] *Ibid.*, para. 11.
[27] Home Office, Data Protection: The Government's Proposals for Legislation (April 1982) 1981/82 Cmnd. 8539, para. 5.
[28] Article 2(d) CPIAPD.
[29] Article 3(1) CPIAPD.

reconciliation of individual and market approaches with a more limited state-facilitative exception than Resolution (74) 29.

The Organisation for Economic Cooperation and Development and Personal Data

In September 1981, the United Kingdom endorsed the Recommendation of the Council of the OECD concerning guidelines governing the protection of privacy and trans-border flows of personal data. The OECD was more clearly driven by market concerns.[30] The preamble to the Recommendation made the removal of trade barriers central to its purpose, recognising "a common interest" in "reconciling fundamental but competing values such as privacy and the free flow of information". The free flow of information required "the development of compatible rules and practices" and could be hindered by national legislation. The Recommendation determined "to advance the free flow of information between Member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among Member countries." The Recommendation's guidelines extended to "personal data, whether in the public or private sectors, which, because of the manner in which they are processed or because their nature or the context in which they are used, pose a danger to privacy and individual liberties."[31] The guidelines were neutral in their application to the public and private sectors: an absence of a public-private divide which is consistent with its market logic.

European Data Protection: Drafting Data Protection Directive 46/95 EC

Market Approaches Tempered by State-facilitative Exemptions

The Data Protection Directive (DPD) shared similar concerns to early European data protection. Jay attributes the Directive to the internal market's need for the free flow of information.[32] The Directive was shaped profoundly by the market approach. Its principles applied to data controllers irrespective of whether they were public authorities or private actors, unless Member States made use of derogations in the implementation of the Data Protection Directive or otherwise legislated consistently with the Data Protection Directive to introduce a national public-private divide.

A state-facilitative influence is also apparent in the text of the Directive. Article 3(2) DPD, on the scope of the Directive, provided that the Directive did not apply to activities "concerning public security, defence, State security (including the economic well-being of the State when

[30] Home Office, Data Protection: The Government's Proposals for Legislation (April 1982) 1981/82 Cmnd. 8539, para. 5.
[31] OECD Recommendation, guideline 2.
[32] Jay (2012), p. 13.

the processing operation relates to State security matters) and the activities of the State in areas of criminal law". This limitation on scope fulfilled a clear state-facilitative objective. Similarly, derogations available under Article 8(4) DPD enabled Member States to make exemptions to the prohibition on processing sensitive personal data for "reasons of substantial public interest". This provision was substantially state-facilitative in application, although of course it was also applicable to processing activities by private data controllers. Article 8(5) DPD made special provision for official control of criminal conviction data. Article 13(1) DPD permitted certain other derogations necessary to safeguard national security; defence; public security; the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters; or a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in certain cases. Although these various derogations are not explicitly limited to public authorities, a state-facilitative approach underpins them. They were drafted primarily with state-facilitative objectives in mind.[33]

All the legal bases for processing data in Article 7 DPD appeared equally available to both public authorities and private actors. There was an additional basis in Article 7(e) DPD for processing "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." Recital 32 DPD provided a state-facilitative explanation for the silence as to the status of such a controller: "it is for national legislation to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public administration or another natural or legal person governed by public law, or by private law such as a professional association." Although Article 7(e) DPD was therefore available to certain private actors, its underlying purpose was to make lawful processing in the public interest or in the exercise of official authority. It was ultimately state-facilitative, although it acknowledged that private actors may contribute to such processing on behalf of the state.

The Role of the Individual Approach in the Development of the Data Protection Directive

A history of the Directive that emphasised only a market approach, tempered by state-facilitative aspects, would neglect the key role of advocates of an individual approach in the

[33] However, there was also a derogation permitting Member States to adopt legislative measures to restrict the scope of certain Articles of the Directive where it was a necessary measure to safeguard "the protection of the data subject or of the rights and freedoms of others": Article 13(1)(g) DPD.

development of the Directive. Pearce and Platten argue that the Directive combined internal market and human rights concerns,[34] although they do argue that it was primarily a response to the failure of early European data protection attempts to "bring about sufficient equivalence to guarantee the free movement of data".[35] Article 1 DPD and the Recitals certainly reflected an attempted reconciliation between privacy and the free flow of information, and with that both individual and market concerns.

However, it is necessary to explain the cause of this "evolution" in the EC's approach to the internal market.[36] As Simitis observes, the Data Protection Directive marked a change in the European Commission's attitude from resistance to support for data protection in order to assist the development of information technology in the internal market.[37] Newman similarly noted that there was resistance at the level of the EC before the 1990s to harmonised data protection.[38] Part of the explanation for this change in attitude was certainly perceived failures of early European data protection to go far enough to harmonise data protection across Europe. However, a fuller explanation also should also note the important role played by advocates of an individual approach in producing this change in the Commission. The strategy of transnational data protection authorities was an important catalyst for the Directive. In this way an individual approach worked to promote legislation which ultimately adopted a more market logic.

Newman argues that national data protection authorities played an "innovative role… in motivating and maintaining supranational action".[39] He argues that this process, rather than integration driven by the interests of firms and States or the Commission, as neoliberal or neofunctional accounts might emphasise respectively, was responsible for the development of the Directive.[40] He argues that the construction of a "European agenda" was the work of a transnational network of data protection authorities, which emerged from bodies created by national legislation in the 1970s.[41] This network was fearful that those countries which then lacked data protection, Belgium, Greece, Italy, Portugal and Spain, would become "data havens" and undercut the regulatory effectiveness of national data protection authorities.[42]

---

[34] Pearce and Platten (1998), p. 532.
[35] *Ibid.*, p. 531.
[36] *Ibid.*, p. 532.
[37] Spiros Simitis, *From the Market to the Polis: The EU Directive on the Protection of Personal Data* (1994-1995) 80 Iowa L Rev 445, 446
[38] Abraham Newman, *Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive* (2008) 62(1) International Organization 103, p. 105.
[39] Abraham Newman, "Privacy Protection in Europe: Administrative Feedbacks and Regional Politics", in Meunier and McNamara (eds.) The State of the European Union (2007), pp. 124 to 125.
[40] Newman (2007), pp. 125 to 126.
[41] *Ibid.*, p. 137.
[42] *Ibid.*, p. 132.

This was because the single internal market permitted greater mobility for data controllers who could choose a more favourable regulatory regime.[43] National data protection authorities therefore lobbied for legislation from the EC.[44] They were concerned about the effectiveness of national regulation in defending individual information rights.

Significantly, on several occasions regulators used national powers to block the flow of information from France and in relation to the Schengen Area,[45] actions that "demonstrated that they could disrupt critical Community goals of integrating the European market and creating a European public administration."[46] The Commission's 1990 proposal for the Data Protection Directive was made in the context of this actual and potential disruption. These threats both to the market and to public administration that were motivated by concerns of the individual approach. It is this further interaction between different approaches that more fully explains the Commission's motivation to initiate legislation at the EC level and to attempt a reconciliation of market and individual approaches.

However, Newman's view is still only a partial explanation for the timing of the Directive proposal. The role of the transnational data protection network and the EC institutions was also facilitated by an earlier reforms in the EC. These reforms themselves reflected a broader market-orientated ambition, albeit not directed at information law in particular. The legal basis for the Directive was Article 100a EC Treaty. This was a new provision introduced three years earlier by the Single European Act 1987 (SEA), an instrument which was aimed at the creation of a truly single internal market in Europe.[47] This was important for European data protection in two respects. First, unanimous voting required by Article 100 Treaty of Rome was replaced with qualified majority voting. Secondly, Article 100a EC Treaty only required measures to "have as their object the establishing and functioning of the internal market", whereas Article 100 Treaty of Rome had required harmonisation to "directly affect the establishment or functioning of the common market". This loosening of the direct link to the internal market helped secure the legal basis for data protection legislation in the EC, although this claim was nevertheless contested and questioned during negotiations.[48] Unanimous voting and a requirement for a direct link would have made the Directive either politically impossible, given opposition to the Directive from some Member States and the questions raised about its legality even under Article 100a EC Treaty, or would have

[43] Newman (2008), p. 113.
[44] Newman (2007), p. 133.
[45] Newman (2008), pp. 103 to 105 and 114 to 116.
[46] Newman (2007), p. 134.
[47] Jay (2012) p. 24.
[48] See, for example, Meetings of the Working Party on Economic Questions (Data Protection), 25 February 1991, para. 9 (Ireland); 27 and 28 March 1991, para. 3 (Belgium); and 2 and 3 May 1991, para. 9.

seriously weakened its provisions. The existence of a broader market focus in the EC therefore framed the ability of national and transnational actors to pursue or resist change in the 1990s. The reform of the EC Treaties to facilitate more legislation directed towards the single market was crucial for the Directive. Such changes were most likely not remotely motivated by concern for data protection but had an important, if unintended or unforeseen, impact on the shape of the law in this field. The Directive was a development that could only have occurred after the SEA 1987.

The influence of data protection authorities, and their agenda with its individual approach, waned during the passage of the Directive. The influence of transnational data protection authorities was much reduced in the negotiations that followed the 1990 Commission proposal itself. These negotiations featured a far greater role for Member State governments, for whom national concerns played a greater role. This tempered the Directive with the state-facilitative demands of Member States. Meanwhile, European institutions, who also played a substantial role, were motivated by a market approach, as were some Member States.[49] Structurally and institutionally, the EC focused more on a market approach once it had been galvanised into action by advocates of an individual approach.

THE 1990 PROPOSAL: A RECONCILIATION OF INDIVIDUAL AND MARKET APPROACHES WITHIN A STATE-RESTRICTIVE FRAMEWORK

Although the 1990 Proposal from the Commission contained a pronounced public-private divide in its structure, reflecting a German model of data protection,[50] it did not survive into the final draft. The resistance to the proposal apparent from Member States and the European Parliament reflects the concerns of a market approach to data protection. Other efforts to temper the Directive with state-facilitative elements were made by some Member State governments. Despite being catalysed by individual and market approaches, the initial proposal was in fact surprisingly state-restrictive, an approach that was fiercely resisted by Member States and European institutions, whose motivations did not lie in state-restrictive or individual approaches but in a mixture of state-facilitative and market concerns.

The recitals to the proposed Directive explained that "the establishment and the functioning of an internal market" required both the free flow of personal data and the safeguarding of fundamental rights.[51] The recitals considered that the "wide variety" of data protection laws and different levels of data protection between Member States "may prevent the

---

[49] See below, pp. 124 to 125.
[50] Pearce and Platten (1998), p. 533; Gloria Gonzalez Fuster, The Emergence of Personal Data Protection as a Fundamental Right of the EU (2014), p. 126.
[51] Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data COM (90) 314 final – SYN 287 90/C 277/03 (27 July 1990), recital 1.

transmission" of data and so ""constitute an obstacle to the pursuit of a number of economic activities at Community level, distort competition and impede authorities in the discharge of their responsibilities under Community law".[52] However, the Directive clearly recognised the importance of the fundamental rights objective of those laws, so that their "approximation… must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community".[53]

Although the initial proposal applied to "files in the public and private sectors" to the extent that they were within the scope of EC law,[54] it distinguished between the public and private sectors.[55] This distinction turned on whether the activities were governed by public law, including the exercise of official authority by an entity governed by private law, or were "industrial or commerce [activities]", including that of public authorities carrying out such activities.[56] Public sector processing was only lawful "in so far as… necessary for the performance of the tasks of the public authority in control of the file", with consent, where pursuant to law, or "in order to ward off an imminent threat to public order or a serious infringement of the rights of others".[57] The communication of personal data from the public sector to the private sector was also lawful for the legitimate interests of a private sector actor which prevailed over the data subject's interest in non-disclosure. This was not available in the context of public sector processing.[58] Requirements of notification and registration with a supervisory authority were limited to the public sector.[59] Processing in the private sector was lawful with consent, carried out under contract or quasi-contract, in the pursuit of a legitimate interest and for using generally accessible data for correspondence.[60] Notification of the data subject was required of private sector actors, unless the communication was required by law,[61] but no registration with a supervisory authority was required.

The original proposal was therefore much more state-restrictive: the public sector could not rely on contract or its own legitimate interests to process, which was not the case in the final Directive. The public sector was limited to public tasks and legal powers even in relation to generally accessible information. Only the public sector was subject to registration with a supervisory authority. This appears to have reflected the position in German law which was

---

[52] *Ibid.*, recital 5.
[53] *Ibid.*, recital 7.
[54] *Ibid.*, Article 3(1).
[55] See *Ibid.*, 2(g) and (h).
[56] See *Ibid.*, Article 2(g) and (h).
[57] See *Ibid.*, Article 5, 6(1)(a) and 6(2).
[58] See *Ibid.*, Article 6(1)(b).
[59] *Ibid.*, Article 7.
[60] *Ibid.*, Article 8.
[61] *Ibid.*, Article 9(2).

considered to be a leader in data protection.[62] Some exceptions did, however, apply in favour of the public sector in relation to the requirement to provide information at the time of collection for certain public functions and the maintenance of public order[63] and to the data subject's right of access to public sector files.[64] Public interest derogations were permitted from the prohibition of processing certain sensitive personal data.[65] The original proposal also sought to confine data concerning criminal convictions to only public sector files, so that only public sector bodies could benefit from it.[66] State-facilitative elements were therefore present even in the Commission's original state-restrictive proposal.

THE EUROPEAN COMMISSION'S MARKET APPROACH

There is little evidence beyond the draft of the proposed Directive that shows the Commission sought a state-restrictive approach. Its other actions point to a market approach to the public-private divide. The Commission explained that the 1981 Convention's "large number of options for… implementation" made it inadequate as a harmonisation measure, especially as only seven Member States had ratified it and only six had implemented it with national legislation.[67] The Commission recalled its earlier recommendation to ratify the 1981 Convention,[68] which reserved the option to "adopt an instrument on the basis of the EEC Treaty" should Member States fail to ratify the 1981 Convention.[69] The resultant diversity had caused "an obstacle to completion of the internal market",[70] although the Commission was silent about the actions of national data protection authorities and their expressed desire to push for such legislation with a commitment to an individual approach. The Commission was also persuaded that harmonisation should go further than the available EC legal powers would permit. The Commission proposed a draft resolution to extend the coverage of the Directive to the public sector when it would not otherwise apply as being outside the scope of the Directive for "the sake of consistency".[71] This was to be implemented via Member States taking national legislative action not otherwise required by the Directive.[72] This

---

[62] Fuster (2014), p. 126.
[63] COM (90) 314 final – SYN 287 90/C 277/03 (27 July 1990), Article 13(2).
[64] *Ibid.*, Article 15.
[65] *Ibid.*, Article 17(2).
[66] *Ibid.*, Article 17(3).
[67] Commission Communication on the protection of individuals in relation to the processing of personal data in the Community and information security (13 September 1990), para. 3.
[68] Commission Recommendation of 29 July 1981.
[69] Commission Communication (13 September 1990), para. 5.
[70] *Ibid.*, paras. 6 and 7.
[71] *Ibid.*, para. 15.
[72] *Ibid.*

reflects a market approach. It is not clear why a state-restrictive approach was prominent in the 1990 proposal beyond the influence of German data protection law.[73]

Resistance to the Proposed Data Protection Directive

Pearce and Platten note that the proposed Directive was controversial and received sustained criticism, especially in relation to the proposed public-private divide.[74] Commentators have suggested that this criticism, and the removal of the public-private divide from the proposed Directive in 1992, was the result of Member State attempts to avoid excessive implementation costs. For example, Pearce and Platten argue that Member States criticism embodied a strategic desire on the part of Member States to ensure that the resulting Directive reflected something of their pre-existing practices and data protection traditions.[75] Simitis similarly argues that the Directive did not reflect a genuine attempt at harmonisation for the sake of common rules but rather reflected Member State interests in preserving their own regulatory traditions.[76] The effect of this political logic was, in his view, to limit the capacity of the Directive to adopt radical changes.[77] They suggest that this struggle limited the development of data protection law: the multiple veto points created by needing to secure Member State support for the proposed Directive resulted in a change in approach. Such narratives align with broader accounts of the role of struggle in the development of information law.

Commenting on the Commission's 1992 revised proposal, Pearce and Platten note that the new text emphasised "the fundamental and more familiar provisions of the [1981 Convention]".[78] It also represented a rebalancing of the influence of different data protection traditions including France, the Netherlands and the UK.[79] Pearce and Platten suggest that the greater French influence was in part the result of CNIL secondments to the Commission as part of a strategy to shape the evolving proposal.[80] This revised proposal met with greater success and support.[81]

I do not doubt that the strategic desire to avoid too drastic a change in the structure of national law motivated some resistance to the original proposal for a Directive. However, an analysis of the preparatory materials for the Directive also reveal substantive criticism of the

---

[73] See Fuster (2014), p. 126.
[74] Pearce and Platten (1998), p. 533.
[75] *Ibid.*
[76] Simitis (1994-1995), p. 449.
[77] *Ibid.*, p. 451.
[78] Pearce and Platten (1998), p. 533.
[79] *Ibid.*
[80] *Ibid.*
[81] *Ibid.*, p. 534.

public-private divide, rooted in a deeper set of concerns about the workability of the Directive as a market measure and the defensibility of the public-private divide it sought to draw. This points to the role of a market approach adopted by some Member States and in the European Parliament as an explanation for the criticism and revision of the original proposal in later drafts. It is therefore mistaken to characterise the 1992 rewrite as the result purely of a clash of Member State interests, based on their pre-existing approach. Instead there was disagreement over the substantive approach itself.[82]

The diversity of Member States' political economies, with a variety different models for the role of public authorities and private actors in providing public services, would mean that a strong public-private divide in data protection at the European level would have produced a lack of harmonisation in different sectors across Europe, depending on whether that sector was a public, private or mixed sector in different Member States. There was also a fear that such a divide would produce uncertainty in application and so undermine harmonisation across Europe. Simitis argues that a clear delineation or limitation to the private sector was impossible, although he considered that the "true area of activity" of the Directive was the market rather than the public sector.[83] These concerns are those of a market approach.

At early meetings of the Working Party on Economic Questions (Data Protection), several Member State delegations questioned the structural public-private divide in the proposed Data Protection Directive.[84] Various delegations pointed to conceptual difficulties in the distinction between public and private sectors and doubted its appropriateness.[85] Some delegations, who did not object to the public-private divide proposed, nevertheless agreed that it should be left to Member States during implementation.[86] However, this view was not universally shared and other Member State delegations supported the divide, arguing that different considerations had to be taken into account in the public and private sectors.[87] There was some diversity of approach and a tension between state-restrictive and market approaches in those discussions. It was not merely an interest-based clash. Principled

---

[82] In 1990, only seven Member States had specific data protection laws (France, Germany, Ireland, Luxembourg, the Netherlands and the United Kingdom): see Commission Communication on the protection of individuals in relation to the processing of personal data in the Community and information security (13 September 1990), p. 15.
[83] Simitis (1994-1995), p. 452.
[84] Meeting of the Working Party on Economic Questions (Data Protection), 25 February 1991, para. 10 (France); Meeting of the Working Party on Economic Questions (Data Protection), 27 and 28 March 1991, paras. 15 (UK and Republic of Ireland), 16 (Denmark) and 17 (France).
[85] Meeting of the Working Party on Economic Questions (Data Protection), 2 and 3 May 1991, para. 13 (Republic of Ireland); Meeting of the Working Party on Economic Questions (Data Protection), 19 and 20 June 1991, paras. 13 (UK) and 14 (France, Greece, Belgium).
[86] Meeting of the Working Party on Economic Questions (Data Protection), 19 and 20 June 1991, paras. 15 (Luxembourg) and 16 (Italy).
[87] *Ibid.*, para. 17 (Spain, Denmark, Germany, Netherlands).

objections were advanced for different approaches. Several objections were made that the measure as proposed could harm the free flow of information and the market more generally. The UK delegation argued that the distinction could cause "practical problems" and interpretation issues in "borderline cases".[88] The French delegation argued that the limits between the public and private sectors were "often unclear", which "would lead to different distinctions being drawn in the different Member States with a consequential distortion of competition".[89]

The European Parliament entirely removed the public-private divide from the structure of the proposed Directive in its proposed amendments of 11 March 1992. In the debates of the European Parliament on 10 February 1992, Geoff Hoon MEP, the rapporteur, explained that there seemed "no good reason to maintain a separation, particularly where in one Member State an organisation might be in the public sector and yet in another Member State an organisation might well be private."[90] He argued that a "common standard for both" was therefore needed.[91] This reflects a market approach to data protection, as it was workability in light of the diversity in European markets and the needs of harmonisation that drove the criticism. On 15 October 1992, the Amended Proposal of the Commission removed the formal public-private distinction from the structure of the proposal and made clear that the level of protection was the same in each sector "at Parliament's request".[92] In this, we can see an acceptance of the principled and practical arguments being advanced by delegations and the European Parliament in favour of a market approach to the Data Protection Directive.

THE ROLE OF MEMBER STATES AND STATE-FACILITATIVE CONCERNS

The Directive was also tempered by a state-facilitative approach in the negotiations. There were repeated attempts by Member State delegations to broaden Article 3(2) DPD, which provided exemptions from the scope of the Directive, and also other derogations that protect core areas of state interest.[93] Struggle therefore played a role here in tempering the Directive according to a state-facilitative approach.

---

[88] Meeting of the Working Party on Economic Questions (Data Protection), 23 and 24 July 1991, para. 3; see also Meeting of the Working Party on Economic Questions (Data Protection), 12 and 13 November 1991, para. 14 (Italy).
[89] Meeting of the Working Party on Economic Questions (Data Protection), 12 and 13 November 1991, para. 13.
[90] Report of the Committee on Legal Affairs and Citizens' Rights, 10 February 1992.
[91] *Ibid.*
[92] Amended Proposal for a Council Directive on the protection of individuals with regard t the processing of personal data and on the free movement of such data, COM(92) 422 final – SYN 287 (15 October 1992), p. 2.
[93] See below, pp. 127 to 129.

The UK delegation expressed discomfort with the proposal to only exclude activities outside the scope of EC law because the UK was concerned that this could result in areas of data processing necessary for national security falling within the shifting definition of EC law.[94] The UK therefore proposed an amendment to add

> without prejudice to the foregoing, it shall not in any event apply to processing which relates to, or otherwise affects, State security, public safety, the monetary interests of the State (including the assessment or collection of public revenues) or law enforcement.[95]

Similar requests were made or supported by some Member States,[96] but opposed by the Commission and others who argued that such provision was too broad.[97] In response to such requests, the Greek Presidency expanded the list of exemptions and restrictions in Article 14 DPD,[98] but resisted the attempt to broaden Article 3(2) and instead proposed a return to wording similar to the original proposal: "in the course of an activity outside the scope of Community law such as data to which Titles V and VI of the Treaty of European Union apply."[99] This proposal was not accepted with various further attempts to substitute alternative wording that excluded public safety, defence, State security, criminal proceedings, State monetary and budgetary interests and public registers.[100] Ultimately, the Greek Presidency indicated a willingness to make concessions despite considering the amendments unnecessary, given the derogations available under Article 14.[101] The Commission also indicated a willingness to agree to many of the exemptions.[102] The consolidated draft of 12 October 1994 adopted new wording in Article 3(2) DPD: "and in any case to processing concerning public safety, defence, State security and the activities of the State in an area of criminal law, excepting the areas which come within Community law".[103]

---

[94] Transmission Note from the UK Delegation to the Working Party on Economic Questions (Data Protection), 31 August 1993, para. 2.
[95] *Ibid.*, para. 7.
[96] Meeting of the Working Party on Economic Questions (Data Protection), 28 and 29 October 1993, para. 2(a) (made by Germany, Denmark, UK, Ireland, France and supported by Netherlands and Italy).
[97] *Ibid.*, para. 2(a) (Belgium, Greece, Spain, Portugal).
[98] Greek Presidency Proposals, 6 January 1994. Article 14 DPD in the negotiations was ultimately renumbered as Article 13 DPD in the final draft.
[99] Presidency Note to Working Party on Economic Questions (Data Protection), 29 March 1994.
[100] Meeting of the Working Party on Economic Questions (Data Protection), 21 and 22 April 1994, para. 2 (supported by UK, Republic of Ireland, France, Denmark, Germany and resisted by Belgium, Spain, Greece and Luxembourg). See also Meeting of the Working Party on Economic Questions (Data Protection), 6 and 7 October 1994, para. 3 (Ireland on public registers).
[101] Note from Presidency to Permanent Representatives Committee, 10 May 1994, para. 10.9.
[102] Report of Permanent Representatives Committee to Internal Market Council, 9 June 1994, para. 2.
[103] Working Document of the General Secretariat of the Council to Delegations, 12 October 1994.

Several Member States,[104] including the UK, objected to this formulation and both Denmark and the UK made further requests for the inclusion of the "economic well-being of the State".[105] The Commission once again resisted and considered that the relevant interests were adequately covered by Article 14 DPD.[106] On 20th February 1995, the Common Position Adopted by the Council adopted wording excluding many areas of State interest from the proposed DPD entirely, including the economic well-being of the State as part of State security under Article 3(2) DPD. This drafting was accepted by the European Parliament on the Data Protection Directive's second reading on 15th June 1995.

In sum, an extensive process of negotiation thereby resulted in the broadening and sharpening of Article 3(2) DPD as part of a reaction by some Member States to protect certain areas of State interest with the potential to cross over with activities within Community law. The wording reflects compromise on the part of those States who felt it unnecessary and reflects the concern of other Member States to protect areas of State interest where the complexity of public-private interaction in those areas made harmonised data protection a threat. The result was a public-private divide shaped in favour of a state-facilitative approach in this regard. It shows a complex interaction between the broader market approach and state-facilitative exemptions preserved in particular areas.

EUROPEAN DATA PROTECTION: THE JURISPRUDENCE OF THE ECJ AND CJEU

The European Court of Justice (ECJ) and Court of Justice of the European Union (CJEU) have moved from a broad market approach to the interpretation of the Directive to an increasingly state-restrictive approach to data protection with a more muted individual approach in relation to processing in the legitimate interests of a (private) data controller where those interests seriously impinge upon Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (CFR). The ECJ and CJEU jurisprudence therefore demonstrates shifts in emphasis between different approaches over time. Although elements of an individual approach have recently arisen, and the courts adopted an earlier market logic, the courts were responsible for a significant sharpening of the public-private divide informed by the resurgence of a state-restrictive approach. This jurisprudential development

---

[104] UK, France, Italy, Ireland: see Working Document of the General Secretariat of the Council to Delegations, 12 October 1994; see also Meeting of the Working Party on Economic Questions (Data Protection), 6 and 7 October 1994.

[105] Working Document of the General Secretariat of the Council to Delegations, 12 October 1994, p. 18; see also Meeting of the Working Party on Economic Questions (Data Protection), 6 and 7 October 1994, para. 3. See also Extract from the Draft Summary Record of the 1628th Meeting of the Permanent Representatives Committee, 17 November 1994; and Report from the Permanent Representatives Committee to Internal Market Council, 30 November 1994, p. 7.

[106] Meeting of the Working Party on Economic Questions (Data Protection), 6 and 7 October 1994, para. 3.

predates the CFR and was based on the reception of Article 8 ECHR jurisprudence into European data protection as a general principle of law. It therefore resembles the developments identified in chapter 3 on European human rights. The effect of fundamental rights in European data protection has been strikingly similar to European human rights.

First, the early jurisprudence concerning the scope of the Data Protection Directive in Article 3(2) DPD reflected clear concerns of the market approach, albeit more at peace with the individual approach aspirations of the Data Protection Directive than Advocate General Tizzano.[107] His Opinions reflected a narrower approach to EC market harmonisation, less influenced by an individual approach. The effect of this early case law was a broad application of the Data Protection Directive to public authorities and private actors, limited only by the express words of Article 3(2) DPD, narrowly construing the state-facilitative exemptions argued for by Member States in the Data Protection Directive negotiations. The sharp public-private divide at the edge of the Data Protection Directive's scope was more a function of the constraint imposed by Article 3(2) DPD's text than of a principled endorsement of that limit by the courts.

Secondly, the jurisprudence developed a state-restrictive approach to processing pursuant to law or in the exercise of official authority, first by subjecting processing under Articles 7(c) and (e) DPD to Article 8 ECHR jurisprudence as a "general principle of law" and later by subjecting such processing to review based on in Articles 7 and 8 CFR, although both share a common structure. This introduced more exacting review of the proportionality of such processing.

Thirdly, the CJEU's recent jurisprudence has extended CFR review to private entities processing data in their legitimate interests under Article 7(f) DPD. Although this reflects the growing importance of an individual approach to the CFR, it lacks the structured approach applied to public authorities. It is more limited in scope.

A Market Approach to the Data Protection Directive but Comfortable with an Individual Approach

In C-465/00 *Rechnugshof v Osterreichischer Rundfunk*,[108] the ECJ held that processing by a public audit body was not exempt from the DPD under Article 3(2) DPD. This was because it neither concerned an activity that fell outside the scope of EC law nor was it a "processing operation concerning public security, defence, State security or the activities of the State in

[107] See below, pp. 130 to 133.
[108] (2003) ECR I-04989 (Judgement) (20 May 2003).

areas of criminal law."[109] The ECJ rejected the suggestion that Article 100a EC Treaty required each situation within the scope of the Data Protection Directive to demonstrate an actual link with the object of the establishment and functioning of the internal market in favour of a more general legislative intention.[110] Therefore, the Data Protection Directive did not require "specific situations" to have a "sufficient link" to the internal market because this would "make the limits of the field of application of the [Data Protection Directive] particularly unsure and uncertain" which was contrary to the "essential objective" of harmonisation to "eliminate obstacles to the functioning of the internal market deriving precisely from disparities between national legislations".[111] The reasoning was fundamentally one of a market approach to justify the broad application of the Directive to public authorities and private actors. The ECJ was confirmed in its view by the breadth of Article 3(1) DPD, the wording of the exemption in first indent of Article 3(2) DPD, and derogations available in Article 8(2) DPD. The ECJ argued that these would not be necessary if the Directive only applied to "situations where there is a sufficient link" with the internal market.[112] No consideration was given to the fact that such wording was only adopted by Member States in fear of such a broad application of the Data Protection Directive.[113]

In C-101/01 *Criminal Proceedings Against Bodil Lindqvist*,[114] the ECJ explained further that the activities listed in Article 3(2) were "in any event, activities of the State or of State authorities and unrelated to the fields of activity of individuals". As a result the "exception applies only to the activities which are expressly listed there or which can be classified in the same category (ejusdem generis)".[115] It could not therefore apply to the charitable or religious activities of Lindqvist. The ECJ applied this reasoning in C-524/06 *Heinz Huber v Bundesrepublik Deutschland* to hold that processing with an "objective… connected with the fight against crime" fell under the first indent of Article 3(2).[116]

The Data Protection Directive therefore applied to all bodies, public or private, with the narrow exception of those *state activities* listed in Article 3(2) DPD. This broad reading of the Data Protection Directive's scope, and narrow interpretation of its exemptions, reflected a market approach constrained only by the explicit wording of Article 3(2) DPD, which was narrowly interpreted. This represents a narrow textual limit on the ECJ's otherwise market approach jurisprudence, reflecting some Member State's State-facilitative approach in that

---

[109] *Ibid.*, para. 45.
[110] *Ibid.*, para. 41.
[111] *Ibid.*, para. 42.
[112] *Ibid.*, paras. 43 and 44.
[113] See above pp. 11 to 12.
[114] See (2003) ECR I-12971 (Judgment) (6 November 2003), paras. 40 and 41.
[115] *Ibid.*, paras. 43 to 45.
[116] (2008) ECR I-09705 (Judgment) (16 December 2008), paras. 44 to 45.

hard fought for exemption. However, despite stating a clear market approach in its reasoning, there is also reason to think that the ECJ was also comparatively relaxed about the individual approach that catalysed the Data Protection Directive and was reinforced by its broad application by the ECJ. This can be seen when the ECJ jurisprudence is contrasted with Advocate General Tizzano's Opinions in *Lindqvist* and *Rundfunk*.

Those Opinions were far more concerned to avoid the broad interpretation of Article 100a EC Treaty that grounded the ECJ's expansive approach to the scope of the Data Protection Directive, although both Opinions shared a commitment to market harmonisation.[117] In *Lindqvist*, the Advocate General's Opinion argued that Lindqvist's processing was outside the scope of EC law because it was "without any intention of economic gain" and was solely ancillary to voluntary work.[118] This non-economic activity had no or no direct connection with fundamental market freedoms, nor was it governed by specific EC laws, and so it fell within Article 3(2) DPD.[119]

Notably, the Opinion also rejected the Commission's argument that "the Directive is not confined to pursuing economic objectives but also has objectives connected with social imperatives and the protection of fundamental rights".[120] The Opinion argued that this was contrived.[121] Advocate General Tizzano argued that to do otherwise than to interpret the Directive in light of its Article 100a EC Treaty legal basis of the establishment and functioning of the single market would call into question the Directive's "very validity".[122] In this regard, the Opinion noted that "no Treaty provision confers on the Community institutions any general power to enact rules on human rights."[123]

In *Rundfunk*, Advocate General Tizzano's Opinion held that a public audit activity did not fall within the scope of the Directive because it was "prescribed and regulated by the Austrian authorities (and in fact in a constitutional law) on the basis of a choice of a policy and institutional nature made by them autonomously and not intended to give effect to a Community obligation," so that it could "only fall within the competence of the Member States."[124] The Advocate General rejected the suggested link argued between Article 141 (sex discrimination), Articles 136 EC and 137 EC (social policy) and the audit activity.[125] He

---

[117] See (2003) ECR I-12971 (AG Opinion) (19 September 2002), paras. 5 to 8.
[118] (2003) ECR I-12971 (AG Opinion) (19 September 2002), paras. 35 and 36.
[119] *Ibid.*, para. 36.
[120] *Ibid.*, para. 38.
[121] *Ibid.*
[122] *Ibid.*, para. 42.
[123] *Ibid.*, para. 43.
[124] (2003) ECR I-04989 (AG Opinion) (14 November 2002), para. 43.
[125] *Ibid.*, para. 45.

also rejected the link between freedom of movement and audit.[126] The Advocate General concluded that the processing was not covered by the Directive because it was "effected in the course of a public activity of audit of accounts which falls outside the scope of Community law within the meaning of Article 3(2) [DPD]."[127] To go any further would entail "a danger of compromising the validity of the [Data Protection Directive] itself, because, in such a case, its legal basis [Article 100a EC Treaty] would clearly be inappropriate."[128]

The Advocate General Opinion in each case showed a clear discomfort with broad interpretations of the Data Protection Directive that would cover a range of non-economic and State activity, considering that to do so would reflect an individual approach to data protection that would call the very legal basis of the Data Protection Directive, and a pure market approach, into question. In light of the contrast with the ECJ's decisions, I suggest that the materials show at least that the ECJ was at peace with the individual approach implicit in such a broad application of the Data Protection Directive, even if the formal reasons given are fundamentally of the market approach. The two approaches are therefore both at work in its reasoning.

A State-Restrictive Approach and Fundamental Rights

Rundfunk was also significant not only for its explicit market approach to scope but for introducing a more state-restrictive approach to processing in compliance with a legal obligation imposed by the State or in the exercise of official authority. The ECJ held that the Data Protection Directive "must necessarily be interpreted in light of fundamental freedoms, which… form an integral part of the general principles of law".[129] It therefore applied Article 8 ECHR to processing undertaken in relation to Articles 6(1)(c), 7(c) and (e) and 13 DPD,[130] albeit that whether the processing was "both necessary for and appropriate" to the aim of the public authority was "a matter for the national courts to examine."[131]

This trend was continued in C-524/06 *Heinz Huber v Bundesrepublik Deutschland*.[132] The ECJ held that the concept of necessity in Article 7(e) DPD, though it had "its own independent meaning in Community law",[133] incorporated the detailed proportionality review characteristic of Article 8 ECHR.[134] The case concerned the processing of personal data

---

[126] *Ibid.*, paras. 46 and 47.
[127] *Ibid.*, para. 49.
[128] *Ibid.*, paras. 54 and 55.
[129] (2003) ECR I-04989 (Judgment) (20 May 2003), para. 68.
[130] *Ibid.*, paras. 70 to 76 and 82 to 83.
[131] *Ibid.*, para. 90.
[132] (2008) ECR I-09705 (AG Opinion) (3 April 2008).
[133] *Ibid.*, para. 52.
[134] *Ibid.*, para. 66.

relating to foreign EU citizens resident in Germany by the Federal Office of Migration and Refugees in a central register to which other public authorities had access.[135] The ECJ held that the "storage and processing of personal data containing individualised personal information… for statistical purposes cannot, on any basis, be considered to be necessary within the meaning of Article 7(e)" because the aim could be achieved with anonymised data alone.[136]

Similarly, in C-92/09 *Volker and Markus Schecke GbR v Land Hessen*, the CJEU applied CFR jurisprudence to Article 7(c) DPD.[137] The case concerned legislation which required the disclosure of personal information relating to the recipients of funds under the Common Agricultural Policy and the balance between transparency and data protection. The judgment marks the first case in which greater emphasis was given to the CFR than Article 8 ECHR. The CFR was signed at Nice in 2000, alongside but not as part of the Treaty of Nice. Articles 7 and 8 CFR address privacy and data protection. This was the result, at least in part, of a "successful lobbying effort" by a former chair of the Article 29 Working Party, Stefano Rodota.[138] The Lisbon Treaty, signed on 13th December 2007 and entering into force on 1st January 2009, gave the CFR the same legal value as the Treaties.[139] Although Article 8 ECHR was cited as legal context,[140] the CJEU held that the national legislation's validity "must be assessed in light of the provisions of the Charter".[141] Article 8(1) CFR was not an "absolute right" but was conditioned by Article 8(2) CFR and could be limited by Article 52 CFR.[142] The CJEU highlighted that "the meaning or scope" of "rights which correspond to rights guaranteed by the [ECHR]" were the same and the CFR did not restrict or adversely affect EHCR rights,[143] so that "the limitations which may be lawfully be imposed on the right to the protection of personal data correspond to those tolerated in Article 8 [ECHR]."[144] The CJEU found that the national legislation interfered with Articles 7 and 8 CFR,[145] and then analysed whether it was justified under Article 52 CFR, which required any interference to be[146]

---

[135] *Ibid.*, para. 1.
[136] *Ibid.*, para. 68.
[137] ECLI:EU:C:2010:662 (Judgment) (9 November 2010).
[138] Newman (2007), p. 135.
[139] Article 6 TEU.
[140] ECLI:EU:C:2010:662 (Judgment) (9 November 2010), para. 3.
[141] *Ibid.*, paras. 45 and 46.
[142] *Ibid.*, paras. 48 to 50.
[143] *Ibid.*, para. 51 to 64.
[144] *Ibid.*, para. 52.
[145] *Ibid.*, paras. 55 to 64.
[146] *Ibid.*, paras. 65 to 71.

> provided for by law, respect the essence of those rights and freedoms, and, subject to the principle of proportionality, necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others.[147]

Increased transparency could be "an objective of general interest recognised by the European Union"[148] but the measure was not proportionate.[149] Less intrusive ways of achieving the aim had not been considered, "such as limiting the publication by name relating to those beneficiaries according to the periods for which they received aid, or the frequency or nature and amount of aid received."[150] An appropriate balance had not therefore been struck.[151]

All these cases focus on Article 7(c) or 7(e) processing and therefore only on processing which is compelled by a legal obligation imposed on the data controller by the state or is processing in for public tasks or in the exercise of official authority. To introduce greater scrutiny in this manner, based on fundamental rights, and not to do so for other grounds of processing under Article 7 DPD, reflects a state-restrictive approach.

Other aspects of European thought reflect a state-restrictive approach. *Schecke* is also notable for the state-restrictive doubts expressed by Advocate General Sharpston about the ability of public authorities to rely on consent as a ground for processing under Article 7(a) DPD. Although the CJEU did not ultimately address this point, Advocate General Sharpston stated that

> as a matter of principle a person applying for funding from a public body such as the European Union (whether the Union is acting alone or jointly with the Member States) cannot be required, solely as a condition of obtaining that funding, to forgo a fundamental right from which he would otherwise derive protection.[152]

As a result, it was irrelevant whether the data subjects had signed application forms on that basis.[153]

The clearest examples of a state-restrictive approach in Articles 7, 8 and 52 CFR jurisprudence can be seen in C-293/12 *Digital Rights Ireland* and C-203/15 *Tele2 Sverige*

---

[147] *Ibid.*, para. 65.
[148] *Ibid.*, para. 71.
[149] *Ibid.*, paras. 72 to 80.
[150] *Ibid.*, paras. 81 to 83.
[151] *Ibid.*, para. 86.
[152] ECLI:EU:C:2010:353 (AG Opinion) (17 June 2010), paras. 85 and 86
[153] *Ibid.*

AB.[154] Although the CJEU has also applied fundamental rights to private data controller processing that infringes Articles 7 and 8 CFR,[155] what is significant is the greater detail and rigour with which these rights were applied to public authority derogations from data protection standards.

In C-293/12 *Digital Rights Ireland*, the CJEU considered the validity of the Data Retention Directive 2006/24/EC (DRD) in light of Articles 7, 8 and 52 CFR.[156] The Data Retention Directive had been proposed in September 2005 following consultation with national law enforcement and sought to harmonise Member State data retention laws for the prevention, investigation, detection and prosecution of criminal offences.[157] The CJEU noted that this was a "wide-ranging" and "particularly serious infringement" of the rights to private life and data protection,[158] as the traffic and location data required to be retained would "allow very precise conclusions to be drawn concerning the private lives of the persons whose data had been retained".[159] The CJEU held that the legislation in question must "lay down clear and precise rules governing the scope and application of the measure… imposing minimum safeguards… to effectively protect… personal data against the risk of abuse and against any unlawful access or use".[160] The CJEU criticised the comprehensive and generalised nature of retention,[161] applicable where there was "no evidence capable of suggesting… a link, even an indirect or remote one, with serious crime" and without exceptions for professional secrecy.[162] The Data Retention Directive was also criticised for lacking a link between the retained data and "a threat to public security", defined by time period, geography, involved persons, or persons whose retained data could contribute to fighting serious crime.[163] It was also criticised for its failure to set "any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use",[164] including "substantive and procedural conditions" relating to that access or use,[165] or limiting the number of persons so authorised "to what is strictly necessary".[166] The absence of "prior review carried out by a court or by an independent administrative body whose decision

---

[154] ECLI:EU:C:2014: 238; [2015] QB 127; ECLI:EU:C:2016:970.
[155] See below, pp. 138 to 140.
[156] [2015] QB 127, para. 23.
[157] *Ibid.*, paras. 11 to 13 and Data Retention Directive, recital 21.
[158] [2015] QB 127, para. 37.
[159] *Ibid.*, para. 27.
[160] [2015] QB 127, paragraph, making explicit analogy with *Liberty v UK* (2009) 48 EHRR 1; *Rotaru v Romania* [2000] ECHR 192; and *S and Marper v UK* (2008) 48 EHRR 1169.
[161] [2015] QB 127, para. 57.
[162] *Ibid.*, para. 58.
[163] *Ibid.*, para. 59.
[164] *Ibid.*, para. 60.
[165] *Ibid.*, para. 61.
[166] *Ibid.*, para. 62.

seeks to limit" access or use "to what is strictly necessary" was also criticised.[167] The CJEU held that the lack of distinction between categories of data based on "possible usefulness for the purposes of the objective pursued or according to the persons concerned" contributed to the Data Protection Directive's failure to be proportionate.[168] Finally, the CJEU held that "the determination of the period of retention must be based on objective criteria in order to ensure that it is limited to what is strictly necessary".[169] The CJEU concluded that the Data Retention Directive did not "lay down clear and precise rules",[170] contain "sufficient safeguards",[171] define the scope of the Data Retention Directive in a "clear and strict manner", or impose "a specific obligation on Member States to establish such rules".[172] Neither did it "ensure the irreversible destruction of the data at the end of the data retention period",[173] or "require the data… to be retained within the European Union".[174] The Data Retention Directive therefore "exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) [CFR]".[175]

In C-203/15 *Tele2 Sverige AB* and C-698/15 *Secretary of State for the Home Department v Watson*, the CJEU addressed the validity of national legislation requiring the retention of data in light of *Digital Rights Ireland*, including the UK Data Retention and Investigatory Powers Act 2014. The CJEU held that the scope of EU law extended to legislative measures "that require… providers to retain traffic and location data, since to do so necessarily involves the processing, by those providers, of personal data"[176] or which relate "to the access of the national authorities to the data retained by the providers of electronic communications services".[177] Such national data retention legislation was a derogation from data protection standards under Article 15 of the Privacy and Electronic Communications Directive 2002/58/EC, which elaborated the requirements of the Data Protection Directive in the electronic communications sector. As with the DRD, derogations applied only "in so far as strictly necessary"[178] and "clear and precise rules" were required on scope and

[167] *Ibid.*
[168] *Ibid.*, para. 63.
[169] *Ibid.*, para. 64.
[170] *Ibid.*, para. 65.
[171] *Ibid.*, para. 66.
[172] *Ibid.*, para. 66.
[173] *Ibid.*, para. 67.
[174] *Ibid.*, para. 68.
[175] *Ibid.*, para. 69.
[176] ECLI:EU:C:2016:970 (21 December 2016), para. 75.
[177] *Ibid.*, para. 76.
[178] *Ibid.*, para. 96.

safeguards.[179] "General and indiscriminate" retention was precluded for the same reasons as in *Digital Rights Ireland*.[180]

What is significant about these judgments is the detailed and demanding nature of the review of legislation they contain. Although the CFR has played a greater role in constraining private data controller processing, private actors procedures and safeguards are not held to similar levels of scrutiny. The CJEU has adopted a state-restrictive approach in its jurisprudence by applying Article 8 ECHR and later Articles 7, 8 and 52 CFR to the Data Protection Directive and more broadly to legislation that enables public authorities to interfere with those rights. Public authorities and private bodies processing at the behest of the state had to undergo a structured and detailed fundamental rights analysis to process data.

THE CHARTER OF FUNDAMENTAL RIGHTS AND PROCESSING IN THE LEGITIMATE INTERESTS OF THE DATA CONTROLLER

Although the CJEU subsequently brought Articles 7 and 8 CFR to bear on processing for the legitimate interests of private actors under Article 7(f) DPD in its more recent decisions, indicating some element of an individual approach, this has not matched the rigorous and structured approach that applies to public authorities, which must also comply with Article 52 CFR.

In C-468/10 *ASNEF v Administracion de Estado*,[181], the CJEU considered whether additional restrictions could be imposed by Member States in relation to Article 7(f) DPD processing in the legitimate interests of the data controller and concluded that they could not,[182] but went on to observe that Article 7(f) DPD still "necessitates a balancing of the opposing rights and interests concerned" and "must take account of the significance of the data subject's rights rising from Articles 7 and 8 [CFR]".[183] Private data controllers reliance on Article 7(f) DPD as a ground of processing was therefore to be tempered by a balancing of their rights and interests with the data subjects' rights in the CFR. However, this is no indication that this is as rigorous or structured as that imposed on public authorities.

---

[179] *Ibid.*, para. 109.
[180] *Ibid.*, paras. 101 to 112.
[181] (2011) ECR I-12181 (Judgment) (24 November 2011).
[182] *Ibid.*, paras. 22, 32 and 39. Although Article 5 DPD did permit Member States to further specify the conditions under which processing would be lawful, subject to being "used only in accordance with the objective pursued by Directive 95/46 of maintaining a balance between the free movement of personal data and the protection of private life" so that it could clarify, but not add additional, requirements: see *Ibid.*, paras. 30 to 36.
[183] *Ibid.*, para. 40.

The CJEU revisited the relationship between Article 7(f) DPD and the CFR in C-131/12 *Google Spain SL v Agencia Espanola de Proteccion de Datos (AEPD)*.[184] The CJEU took a more robust approach to the protection of fundamental rights against private data processing and characterised the objective of the DPD as "ensuring effective and complete protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data" so that the Data Protection Directive could not be "interpreted restrictively".[185] The Data Protection Directive was to "ensure a high level of protection of the fundamental rights and freedoms of natural persons,"[186] and

> in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must necessarily be interpreted in light of fundamental rights, which, according to settled case-law, form an integral part of the general principles of law whose observance the Court ensures and which are now set out in the Charter.[187]

The CJEU observed that search indexing and disclosure to third parties on a personal name search by a search engine operator could significantly affect individual privacy and data protection rights, an effect "heightened on account of the important role played by the internet and search engines in modern society, which render the information contained in such a list of results ubiquitous."[188] This led the CJEU to hold that "it is clear that it cannot be justified by merely the economic interest which the operator of such an engine has in that processing."[189] The CJEU furthermore concluded that the data subject's rights in such a context overrode, "as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information upon a search relating to the data subject's name", subject to certain instances of "preponderant" public interest.[190]

This undoubtedly marks a new phase in the CJEU's jurisprudence, whereby a more robust approach has been adopted to secure the fundamental rights of the data subject, not merely against public authorities, but also against powerful private data controllers acting in their legitimate interests. However, there remains a difference in that the analysis is one of balancing rights rather than the more detailed and structured analysis applied to processing

---

[184] ECLI:EU:C:2014:317 (Judgment) (13 May 2014).
[185] *Ibid.*, para. 53.
[186] *Ibid.*, para. 66.
[187] *Ibid.*, para. 68.
[188] *Ibid.*, para. 80.
[189] *Ibid.*, para. 81.
[190] *Ibid.*, paras. 97 to 99.

pursuant to public power. Although the individual approach has become more influential in the CJEU jurisprudence, there is a more significant ongoing role for state-restrictive thinking.

European Data Protection: Legislative Reforms after Lisbon

A General Data Protection Regulation (GDPR) was proposed by the European Commission in 2012 as part of a package of data protection reforms in the EU. It made use of the new legal basis in Article 16 TEU created by the Treaty of Lisbon.[191] The GDPR was passed on 25th May 2016 to come into force on 25th May 2018. The GDPR and its negotiations indicate the increased role of an individual approach, building upon the market approach, but with both state-restrictive and state-facilitative approaches more influential in the final text. The GDPR is therefore the result of the interaction of all four approaches. It does not represent straightforwardly the rise of an individual approach, nor a mere struggle between different approaches. In particular, the GDPR introduces a much starker state-restrictive public-private divide in the lawful bases for processing. It marks a resurgence of the state-restrictive approach alongside the acceptance of a baseline market approach, the endurance of state-facilitative exemptions and significant increases in protections for individuals.

Development of the Market and Individual Approaches

Jay observes that Article 16 TEU marked the moment at which a clear legal basis came into existence for data protection in its own right "rather than as a single market measure".[192] However, although the way was open to adopt an individual approach openly, considerations of a market approach remained highly influential. In 2012, the Commission sought greater harmonisation, arguing that the Data Protection Directive had "not prevented fragmentation in the way personal data protection is implemented across the Union".[193] Reform was needed to build "trust in the online environment",[194] as there was a "widespread public perception that there are significant risks associated notably with online activity", which was a key reason for "a stronger and more coherent data protection framework in the EU".[195]

The GDPR continued the market harmonising project of the Data Protection Directive, considering its objectives and principles "sound" though the Directive had failed to prevent "fragmentation" in the implementation of data protection across the EU.[196] It was feared that

---

[191] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012) 11 final (25 January 2012).
[192] Jay (2012), p. 38.
[193] COM(2012) 11 final (25 January 2012), explanatory memorandum, para. 1.
[194] *Ibid.*
[195] *Ibid.*
[196] Recital 7 GDPR.

this "may prevent the free flow of information" and "constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities".[197] The GDPR indicated that building the "trust that will allow the digital economy to develop across the internal market" was an important objective.[198]

On the other hand, an individual approach is far more explicit in the GDPR. The Recitals to the proposed draft GDPR highlighted its basis in fundamental rights.[199] The final GDPR emphasised the protection of personal data as a "fundamental right",[200] in the context of the "exchange of data between public and private actors"[201] and technological change and globalisation that enable "both private companies and public authorities to make use of personal data on an unprecedented scale".[202] The notion of fundamental rights of individuals, relevant against both public and private actors reflects thinking associated with an individual approach. The GDPR puts in place an extremely strong set of enforcement powers, especially in relation to large private undertakings. The GDPR provides for administrative fines of the highest of 10 million[203] or 20 million euro[204] or, for undertakings, 2%[205] and 4%[206] respectively of total worldwide annual turnover of the preceding financial year, depending on the provision of the Regulation breached. These levels are significantly higher than in the original draft and target large private companies. An undertaking would need a total worldwide annual turnover of 500 million euro to be affected by the higher limit provided for by the percentage provisions. This marks a significant shift towards an individual approach, especially in respect of substantial enforcement powers against both public and private actors.

STATE-FACILITATIVE DIMENSIONS OF THE GDPR

Several state-facilitative exemptions in the GDPR mirror those in the Data Protection Directive. Article 2(2)(a)(c) GDPR excluded processing "by the Member State when carrying out activities which fall within the scope of Chapter 2 or Title V of the Treaty on European Union". Various exemptions and restrictions in the GDPR concern crime and public

---

[197] *Ibid.*
[198] Recital 6 GDPR.
[199] Recital 1 GDPR.
[200] Recital 1 GDPR.
[201] Recital 4 GDPR.
[202] Recital 5 GDPR.
[203] Article 79(3) GDPR.
[204] Articles 79(3)(a) and 79(3)(aa) GDPR.
[205] Article 79(3) GDPR.
[206] Articles 79(3)(a) and 79(3)(aa) GDPR. See also Recital 120 GDPR.

security,[207] the independence of the judiciary,[208] tax, finance, regulation.[209] GDPR provides for various derogations subject to detailed legislation and necessity and provided they are proportionate in a democratic society, many of which are state-facilitative in nature, although derogations for the safeguarding of the rights and freedoms of others are also listed.[210]

The GDPR also contains a number of other state-facilitative exemptions that were not present in the Data Protection Directive. Many of these exemptions function to protect public authorities from the full force of the Regulation's provisions and were not in either the Commission's proposal or the European Parliament's position document following the first reading. Instead, they were introduced as part of the Council's General Approach on 15th July 2015, late in the negotiations. This suggests that they were concessions to obtain Member State support for the GDPR. To that extent, state-facilitative exemptions reflect struggles by Member State governments, as they did in the Data Protection Directive. For example, the right to erasure does not apply to the extent that processing is based on Article 6(c) or (e) GDPR.[211] Neither does the right to data portability apply to such processing,[212] as that right "by its very nature… should not be exercised against controller processing data in the exercise of their public duties".[213] Nor does the right to object apply to certain processing necessary for a task carried out in the public interest.[214] Measures relating to profiling do not apply if the decision is "authorized by Union or Member state law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests",[215] although exemptions also apply in the case of contract or explicit consent.[216] The monitoring of approved codes of conduct under Article 38a GDPR does not apply to processing carried out by public authorities and bodies.[217] The obligation to have representatives where a controller is not established in the Union does not

---

[207] See Recital 16 GDPR.
[208] See Recital 16a GDPR.
[209] See Recital 24c GDPR. See also Recitals 42 and 59 GDPR.
[210] Article 23 GDPR. The areas that may be safeguarded in this way are national security, defence, public security, the prevention, investigation, detection or prosecution of criminal offences, or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security, other important objectives of general public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or a Member State, including monetary, budgetary and taxation matters, public health and social security, the protection of judicial independence and judicial proceedings, the prevention, investigation, detection and prosecution of ethics for regulated professions, a monitoring, inspection or regulatory function connected to the exercise of official authority, the protection of the data subject or the rights and freedoms of others, the enforcement of civil claims.
[211] Article 17(3)(b) GDPR.
[212] Article 18(2a) GDPR; see also Recital 55 GDPR.
[213] Recital 55 GDPR.
[214] Article 21(6) GDPR.
[215] Article 20(1a)(b) GDPR.
[216] Article 20(1a)(a) and (c) GDPR.
[217] Article 38(a)(6) GDPR.

apply to a public authority or body.[218] The GDPR also permits Member States to lay down rules on "whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State",[219] creating a substantial opportunity for Member States to remove the most powerful enforcement measure from application to public authorities.

Other State-facilitative elements are directed towards shielding public bodies from the regulatory or judicial oversight of the supervisory authorities or courts of other Member States, reflecting the potential political sensitivities that accompanied a more integrated enforcement apparatus. Only the supervisory authority of the Member State is competent where processing is carried out by a public authority or private bodies acting on the basis of Article 6(1)(c) or (e) GDPR[220] and provisions on lead supervisory authorities do not apply.[221] The right to a judicial remedy against a controller or processor "may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers",[222] in which case it must be done in the State of the public authority.

Finally, other differences in treatment reflect the differences between the legislative process for public authorities and decision-making in private bodies. Data protection impact assessments are not required where processing is pursuant to Article 6(1)(c) and (e) GDPR and a "data protection impact assessment has already been made as part of a general impact assessment in the context of the adoption of this legal basis… unless Member States deem it necessary to carry out such assessment prior to the processing activities."[223] The GDPR therefore contains a substantial number of provisions, beyond those found in the GDPR, which reflect the state-facilitative agenda of Member States.

STATE-RESTRICTIVE DEVELOPMENTS IN THE GDPR

The GDPR also attempted to elaborate and sharpen the requirements of the public-private divide to reflect a more state-restrictive approach, although this did not survive the negotiation process in all respects. For example, a Recital in the original proposal stated that consent could not be used as a basis for processing where a "clear imbalance" existed, which would be the case where the controller was a public authority and could "impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely

[218] Article 25(2)(c) GDPR.
[219] Article 79(3)(b) GDPR.
[220] Article 51(2) GDPR.
[221] See Article 51A GDPR; Recital 98 GDPR.
[222] Article 75(2) GDPR; see also Recital 116 GDPR.
[223] Article 33(5) GDPR; see also Recital 73 GDPR.

given, taking into account the interest of the data subject".[224] However, in the final draft, this was changed to "where the controller is a public authority and this makes it unlikely that consent was freely given in all the circumstances of that specific situation."[225]

The state-restrictive approach is clearest in Article 6 GDPR. The provision sets out on the grounds for lawful processing. Articles 6(1)(c), (e) and (f) GDPR replicate Articles 7(1)(c), (e) and (f) DPD respectively. Article 6 GDPR expressly provides that Article 6(1)(f) "shall not apply to processing carried out by public authorities in the performance of their tasks". Recital 38 GDPR clarified that this was because "it is for the legislator to provide by law the legal basis for public authorities to process data". Public authorities therefore cannot rely on their legitimate interests to process personal data without a legal basis. There is some uncertainty over whether this means that public authorities can never rely on legitimate interests, as was the case in the rejected 1990 proposal for the Data Protection Directive, or whether this is limited to public authorities when carrying out their tasks qua public authorities.[226] Article 6(3) GDPR elaborates that the legal basis "may contain specific provisions to adapt the application of rules of this Regulation", including "general conditions governing lawfulness"; the types of data, data subject, recipients and purposes that may be disclosed; "purpose limitation"; "storage periods and processing operations and processing procedures". Article 6(3) GDPR also requires that the relevant law "meet an objective of public interest and be proportionate to the legitimate aim pursued". The GDPR does much to subject public authorities to tighter standards of legality by removing the option to rely on the open-ended legitimate interests clause when carrying out public authority tasks.

The GDPR also creates a more extensive role for data protection officers in the public sector. Data protection officers are required in any case where processing is carried out by a public authority or body, except for courts in their judicial capacity,[227] and only where the processor is a private body in more circumstances, where a controller's or processor's core activities required "regular and systematic monitoring of data subjects on large scale" or consisted large scale processing of special category personal data or personal data relating to criminal convictions and offences.[228]

---

[224] See original Recital 34 GDPR in Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012) 11 final (25 January 2012).
[225] Recital 34 GDPR.
[226] Oliver Butler, Obligations Imposed on Private Parties by the GDPR and UK Data Protection Law: Blurring the Public-Private Divide (2018) 24(3) European Public Law 555.
[227] Article 35(1)(a) GDPR.
[228] See Article 37 and Recital 97 GDPR.

The GDPR therefore restricts to some extent processing by public authorities based on consent, although not as much as in the original draft, and completely based on legitimate interests, which had been a widespread ground, if controversial, for public sector processing under the 1995 Directive. The effect was to insist much more clearly on detailed legislation as the basis for processing by public authorities, following a state-restrictive approach to public authorities' processing.

THE EXPANSION OF EU DATA PROTECTION IN THE FIELD OF POLICE AND CRIMINAL MATTERS

In December 2015, political agreement was reached on a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (PCMD). Such processing was exempted from the GDPR under Article 2(2)(a)(e) GDPR. The PCMD applies to the processing of competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and the prevention of threats to public security.[229] It extends in substance many of the provisions of the Data Protection Directive to such competent authorities, although it does not preclude higher safeguards.[230] Competent authorities include "any other body or entity entrusted by national law to exercise public authority and public powers for the purposes of this Directive"[231] and so is not limited to traditional public authorities, such as the police, but potentially private bodies entrusted with such functions. It does not apply to activity falling outside the scope of Union law, expressly national security activities and issues.[232] These developments show the expansion of EU data protection in relation to police and criminal matters over time to activities that were exempt from the scope of the Data Protection Directive. It therefore marks a more state-restrictive approach to police and criminal matters in European data protection.

COMPLEX INTERACTIONS BETWEEN DIFFERENT APPROACHES: THE PUBLIC-PRIVATE DIVIDE IN EUROPEAN DATA PROTECTION

The history of the public-private divide in European data protection law is a complex one in which the four approaches to the public-private divide have interacted, resulting in various compromises and mixed approaches.

---

[229] Articles 1(1) and 2(1) GDPR.
[230] Article 1(1a) GDPR.
[231] Recital 11 PCMD.
[232] Recital 11b and Article 2(3) PCMD.

An individual approach has undoubtedly risen in importance. A market approach has subsisted throughout the history of the public-private divide in data protection. State-facilitative approaches have endured in the exemptions afforded to public authorities. A state-restrictive approach, both through the courts and GDPR, has resurged in importance alongside greater concern for individual rights against private actors. European data protection is important in demonstrating the complex interactions between the approaches that have shaped the public-private divide. The rejection of state-restrictive approaches to respect for private life in ECHR jurisprudence, motivated by an individual approach, gave rise to threats to the free flow of data that produced market-driven data protection. This was true of both the 1981 Convention and the Data Protection Directive. Market and state-facilitative approaches prevailed over state-restrictive drafting and individual ambitions in the Data Protection Directive. The state-restrictive, and to a lesser extent individual, approaches influenced the later jurisprudence of the ECJ and CJEU. Finally, the individual approach was a major influence on the GDPR which nevertheless contains a resurgence of state-restrictive and endurance of state-facilitative elements.

Throughout, the enduring and complex interaction of market, individual, state-restrictive and state-facilitative approaches is apparent and important for understanding the shape of the public-private divide in European data protection law. It contradicts the suggestion that data protection is inevitably converging on a single individual approach to the public-private divide or is the mere fruit of struggle between different approaches.

CHAPTER 6

THE PUBLIC-PRIVATE DIVIDE AND UK DATA PROTECTION

INTRODUCTION

National data protection law developed in the United Kingdom in response to developments at the European level, although the UK was a reluctant adopter of European data protection norms and frequently diverged from the European approach. This chapter examines the development of the public-private divide in UK data protection law. It argues that national data protection, though broadly driven by European developments, also demonstrates divergence of approach. Complex interactions between the four approaches to the public-private divide can be identified in the development of this field. It does not show a gradual shift from a state-restrictive to an individual approach and, although tensions and struggles sometimes produce divergence, a picture more complex than struggle alone emerges.

Although UK data protection law to 2017 was largely driven by European developments, there were important examples of divergence in national implementation driven by differences in approach to the public-private divide.[1] Parliament legislated in response to European data protection law in 1984 and 1998. The UK was a relatively reluctant adopter of European data protection law. Its implementation of that law demonstrated a stronger emphasis on a market approach than European law. UK Governments were also

[1] In 2018, Parliament passed the Data Protection Act 2018, which repealed the Data Protection Act 1998 in preparation for the coming into force of the General Data Protection Regulation on 25 May 2018. The Data Protection Act 2018 falls outside the scope of this thesis, which analyses the period from 1948 to 2017. As it was drafted after the decision had been taken to notify the EU of the UK's intention to withdraw, Brexit-related considerations, which are still evolving and uncertain at the time of writing, shaped the drafting of the Act and mark it as a development outside the distinctive period of European influence examined in this thesis. See chapter 1, p. 9. Two significant aspects of state-facilitative development related to implementing the GDPR may be briefly noted. First, Parliament sought to soften the effect of Article 6 GDPR by narrowly defining a body as a "public authority" only when "performing a task in the public interest or in the exercise of official authority": Data Protection Act 2018, s. 7(2). For a recent analysis of this development, see Oliver Butler, *Obligations Imposed on Private Parties by the GDPR and UK Data Protection Law: Blurring the Public-Private Divide* (2018) 24(3) European Public Law 555. Secondly, the Act exempted a number of provisions of the GDPR where the provisions are "likely to prejudice" either "the maintenance of effective immigration control" or "the investigation or detection of activities that would undermine effective immigration control": Data Protection Act 2018, Sch. 2, para. 4. This represents a very broad state-facilitative exemption that was not present in the Data Protection Act 1984 or Data Protection Act 1998. It received substantial criticism and is likely to be the subject of a judicial review challenge for incompatibility with the GDPR. See Liberty, Abridged Briefing on the Data Protection Bill 2017: The Immigration Control Exemption (December 2017); see also Open Rights Group, What is at Stake with the Immigration Exemption Legal Challenge?,https://www.openrightsgroup.org/blog/2018/what-is-at-stake-with-the-immigration-exemption-legal-challenge (3 August 2018). The Data Protection Act 2018 was therefore used as an opportunity to soften the state-restrictive provisions of the GDPR. It was, however, more restrictive of processing by the state outside the scope of European law, including new provisions on intelligence services processing: see Data Protection Act 2018, Part 4.

unpersuaded by individual and state-restrictive approaches in this field and have pursued state-facilitative and market approaches to national implementation. Although Europeanisation required an increasingly individual approach, there is little evidence that it was important to most UK institutions, with the exception of the Information Commissioner's Office (ICO). However, the UK also developed a public-private divide divergent from European data protection law with a state-restrictive approach in two particular areas. The main causes of this were a state-restrictive approach inherent in freedom of information jurisprudence and the national response to major data breaches by public authorities in 2008. The market approach, albeit present in European data protection, has been stronger at the national level. Successive UK Governments have also pursued state-facilitative objectives, although these have largely been resisted by Parliament.

National data protection law in the UK largely owes its existence and shape to European developments but, within the broad outline set by those developments, distinctive national trends have emerged in the public-private divide. Attempts to increase transparency[2] and restore public trust in the public sector[3] both contributed to the development of the public-private divide in national law. These trends contradict analyses which anticipate the erosion of a state-restrictive public-private divide in favour of an individual approach. They also show the resurgence of state-restrictive concerns at the national level after 2008, diverging from European data protection law. Relatively unwelcome to business or Government interests, development of data protection law has also been grudging and more market-orientated outside these pockets of state-restrictive development. Government, Parliament and the national courts have all contributed to such developments, creating a public-private divide that diverged from European data protection law both by being more firmly market-orientated and later by introducing features which reflect a more State-restrictive approach.

Initially, UK Governments were resistant to data protection in the public sector and apathetic to regulation in the private sphere. This reflected a set of state-facilitative and market approaches. Regulation was considered unnecessary in the public sector and a threat to developing technologies in the private sector. Several attempts to pass legislation in the 1970s failed to secure parliamentary backing and Government support. However, there was sufficient concern to commission reports on the regulation of information, which reflected the existence of more individual approaches to the public-private divide, although these failed to shape the law. The UK Government's limited embrace of data protection in 1984 reflected, in large part, a strong acceptance of the market approach in European data protection. It

[2] See below, pp. 160 to 165.
[3] See below, pp. 165 to 166.

sought to fulfil its international obligations under the 1981 Convention of the Council of Europe. The development of European law drove UK law, which followed a similar approach. The later Data Protection Act 1998 implemented the European Communities Data Protection Directive 1995. It broadly reflected the approach developed in the 1995 Directive and contained exemptions as permitted by the Directive, but in several respects was more market-friendly. This points to a greater market approach in UK implementation than the Directive and divergence of approach.

By contrast, developments after 2000 show more divergence from this approach in two important respects, each marking the resurgence of a more state-restrictive approach. First, freedom of information legislation extended subject access request rights against public authorities and resulted in the greater disclosure of official personal data. The national courts and the Information Tribunal developed the public-private divide in information law in their jurisprudence on fair processing in the context of the application of section 40(2) Freedom of Information Act 2000. This provides an absolute exemption from FOI disclosure for personal data where the release of the data would violate one or more of the data protection principles. Fair processing, which is the first data protection principle, was interpreted in light of notions of transparency and accountability to introduce a state-restrictive divide in relation to public officials' personal data.[4] In elaborating the detail of data protection, this resulted in divergence from the broader approach seen in the Data Protection Directive and the Data Protection Act 1998. Secondly, a public-private divide in the Information Commissioner's Office's (ICO) enforcement powers was also developed in line with a state-restrictive approach by both Government and Parliament. In large part, those reforms were a Government response to a major HMRC data breach in late 2007 and other breaches in the public sector. Failures of public authorities prompted the introduction of more state-restrictive enforcement powers in Parliament. Advocates of other approaches shaped this law or engaged in struggles over it. The Government's approach also reflected the resistance of business leaders to increased regulatory burdens. These reforms considered and rejected the ICO's individual approach to its enforcement powers. The reforms were driven by a perception that public trust needed to be restored in public bodies' data handling to facilitate their wider activities. However, the reforms in the Coroners and Justice Act 2009 were themselves part and parcel of a wider set of reforms promoted by the Government with a state-facilitative ambition. It was parliamentary resistance to the breadth of those reforms that resulted in the Government abandoning the state-facilitative aspects, leaving the state-

[4] See below, pp. 162 to 164.

restrictive approach behind.[5] This is an important example of multiple approaches interacting in complex ways across diverse actors in order to produce the public-private divide found in UK information law. The ultimately state-restrictive amendments were in fact part of a broader state-facilitative legislative agenda of UK Governments, which Parliament successfully resisted.

Although the ICO pushed for greater transparency in the public sector, with some impact on data protection, it consistently rejected the notion that a public-private divide was justified in the scope of its enforcement powers. It argued to remove any such divide.[6] However, this individual approach failed to influence the two major developments identified in this chapter.

These later developments in the history of the public-private divide in UK data protection mark something of a later resurgence of state-restrictive elements driven by a wider concern for transparency in the public sector and reactions to prominent public-sector data protection failures. Different approaches have been favoured or prioritised by Government, Parliament, the courts and the ICO. The existing data protection framework therefore reflects complex interactions between different approaches adopted by diverse national actors, albeit somewhat constrained by the broader framework designed by European institutions. In the history of the public-private divide in UK data protection law we therefore see the tensions, conflicts and changing fortunes of the four approaches that have shaped the law in this area.

Early Government Resistance to Data Protection

There were attempts by Members of Parliament in the late 1960s and 1970s to pass data protection legislation. These attempts usually took the form of Private Member Bills. They reflected individual approaches to the public-private divide, motivated by a concern to protect individual rights from developing technologies. However, they failed to attract Government support. For example, the Data Surveillance Bill 1969 sought to "prevent the invasion of privacy through the misuse of computer information" by establishing a register of data banks and a right to apply for the amendment of or expunging data,[7] backed by both criminal penalties and damages liability.[8] The Personal Records (Computers) Bill 1969 and Control of Personal Information Bill 1971 both made further attempts to control data banks and protect individuals. As Jay notes, these attempts had "no real hopes of success".[9] None of the attempts came to fruition because Governments were either indifferent or hostile to data

[5] See below, pp. 165 to 170.
[6] See below, pp. 170 to 173.
[7] See Data Surveillance Bill 1969, cl. 5.
[8] See Data Surveillance Bill 1969, cls. 6 and 7 respectively.
[9] Rosemary Jay, Data Protection Law and Practice (2012), pp. 4 to 5.

protection regulation, for reasons that reflected the logic of either state-facilitative or market approaches to the public-private divide.

Although this minority of concerned advocates made little legislative impact, their efforts helped to promote research and reports in the field of data protection and privacy. Jay notes that it was the "impetus" of these early attempts that led the Wilson Labour Government to appoint Kenneth Younger in May 1970 to lead a Committee on Privacy.[10] The Wilson Government lost the General Election in June 1970 and as a result the Younger Committee reported to the Heath Conservative Government in 1972.[11]

There were attempts by the Government to limit the ability of the Younger Committee to propose reforms that would affect the public sector. This reflected a state-facilitative attitude within Government. The Younger Committee's terms of reference were expressly limited to data protection in the private sector.[12] The Government gave three reasons for shielding the public sector in this way. The first was a view that the public sector was sufficiently regulated by existing law: "the scope of [local authority and public corporation] operations was already governed by statute".[13] The second was that the public sector was subject to political control and so had less need for additional legal controls because "they were already answerable for their conduct either directly or indirectly to the electorate".[14] The final reason was that separate reforms were "being contemplated in relation to public authorities".[15] These reasons have in common a desire on the part of the executive to maintain political control over the regulation of information in the public sector. The reasons resisted leaving open the possibility of recommendations by an independent Committee, which could propose further legal controls on the public sector. I therefore suggest that the motivation behind these limited terms of reference was a state-facilitative approach on the part of the Government.

The Younger Report was inhibited but not defeated by its terms of reference. In this, a more individual approach may be discerned. It made detailed recommendations including a series of reforms to press regulation, broadcasting, credit reference agencies, banks, employment, universities, medicine, private detectives, technical surveillance devices, computers and confidentiality, including personal information principles for computer use.[16] The Younger Committee could not give similarly detailed proposals for the public sector but nevertheless recommended that the "Government should consider the possibility of including both the

---

[10] *Ibid.*
[11] Home Office, Data Protection: The Government's Proposals for Legislation (April 1982) 1981/82 Cmnd. 8539, para. 2.
[12] Younger Report, para 1; Jay (2012), p. 5.
[13] Younger Report, para. 4.
[14] *Ibid.*, para. 4.
[15] *Ibid.*
[16] *Ibid.*, paras. 45 to 55.

public and private sectors within the purview of a standing commission to receive complaints about violations of privacy".[17] The Younger Committee's concern to protect individuals across the public-private divide demonstrates an individual approach in tension with the state-facilitative approach of the Government.

In part in response to the Younger Report, the second Wilson Labour Government in 1975 addressed the regulation of information in two papers: Computers and Privacy[18] and Computers: Safeguards for Privacy.[19] Computers: Safeguards for Privacy was a small supplementary report on the public sector in the UK written to "parallel" the Younger Committee's review of the private sector, with the work conducted by an interdepartmental working party made up of government officials.[20] Again, this suggests an attempt to shield the public sector from the independent Younger Committee in favour of executive control over policy formation and a state-facilitative motive at work. Turning to the Computers: Safeguards for Privacy White Paper, the Government stated that it was not persuaded that a significant problem existed in relation to information generally, and certainly not in the public sector, which it strenuously defended. In adopting this perspective, it demonstrated at highest support for a weak market approach underpinning its conclusions. This was supported by a strong state-facilitative ambition that found common cause with the low level of regulation promoted by a weak market approach. First, the Government doubted the significance of purported problems with information law in the public sector. For example, the Government emphasised that development in information technology had resulted in merely "increasing *concern*… about actual or potential threats to the privacy of the individual".[21] It did not acknowledge the validity of such concerns but rather questioned their evidential basis. The Government argued that the White Paper's research "discloses no evidence to suggest that fears about the improper use of computers in the public sector are justified by present practice".[22] The Government also doubted the possibility of potential threats to individual privacy and argued that "substantial safeguards against the realisation of any such fears" existed.[23] The Government's position did not accept that computers posed a risk to privacy in the public sector. It noted that computers reduced the number of potential human contacts with the data, reduced errors and opportunities for information to be inadvertently disclosed and in fact "concluded that the introduction of computer systems would in no way increase the threat to privacy by unauthorised disclosure of personal information held in the

---

[17] *Ibid.*, paras. 54 and 628.
[18] Home Department, Computers and Privacy, Cmnd 6353 (1975).
[19] Home Department, Computers: Safeguards for Privacy, Cmnd 6354 (1975).
[20] *Ibid.*, para. 3.
[21] Home Department, Computers and Privacy, Cmnd 6353 (1975), para. 1 (emphasis added).
[22] *Ibid.*, para. 2.
[23] *Ibid.*

systems."[24] The Government also commented that the "quality of record keeping in a computer system is almost always higher than in a manual system."[25] It was similarly confident about the ability of local government to protect information,[26] considering that effective safeguards were in place.[27] However, despite this, the Government ultimately accepted the need for legislation to "seek to secure that all existing and future computer systems in which personal information is held, in *both the private and public sectors*, are operated with appropriate safeguards for the privacy of the subject of that information".[28] This response was consistent with the market approach, conceding a low level of protection for the sake of promoting sufficient trust in new technologies. This approach of the Government in 1975, generally sceptical of the need for data protection but willing to countenance a low level of protection to secure confidence in both the public and private sector, was an attitude that reflects a market approach consistent with state-facilitative aims.

A policy focus on both public and private sectors was reinforced by the Lindop Committee. In July 1976, during the Callaghan Labour Government, the Lindop Committee was established to consider both the public and private sectors.[29] In December 1978, the final report[30] of the Lindop Committee recommended regulation in both sectors.[31] The Lindop Report recommended a "Data Protection Act" to cover the "automatic handling of… personal data", requiring data handlers to ensure "adequate safeguards for the interests of data subjects", and to comply with a set of data principles and a scheme of registration.[32]

The pressure of growing concerns for data protection, which favoured an individual approach, therefore resulted in a weaker market-orientated compromise from Governments in the 1970s at the level of policy formation. However, no legislative action was successful to implement these recommendations in the 1970s. It was in fact the activity of European institutions and market pressure that was to cause the Thatcher Conservative Government to first legislate for national data protection in the 1980s, in line with a market approach, rather than national pressure to legislate.

---

[24] Home Department, Computers: Safeguards for Privacy, Cmnd 6354 (1975), para. 11.
[25] *Ibid.*, para. 13.
[26] *Ibid.*, para. 54.
[27] *Ibid.*, para. 57.
[28] Home Department, Computers and Privacy, Cmnd 6353 (1975), para. 4 (emphasis added).
[29] Jay (2012), p. 6.
[30] Lindop Committee Report Cmnd 7341 (1978).
[31] Jay (2012), p. 6.
[32] Lindop (1978), Ch. 38.

National pressure to adopt data protection legislation was ultimately overtaken by the concern that a lack of harmonised regulation risked creating barriers to trade, both in Europe and internationally. Jay writes that in the 1980s "the threat of trade barriers galvanised the government of the day into action".[33] The development of European data protection, notably the 1981 Council of Europe Convention, and fears that individual States would block UK data flows, encouraged the Conservative Government to propose legislation.[34]

The 1982 White Paper, Data Protection: The Government's Proposals for Legislation,[35] followed a statement of the Home Secretary on 19 March 1981 announcing the UK Government's intention to introduce legislation on data protection. The Government claimed that the legislation was both a response to "the threat to privacy posed by the rapid growth in the use of computers" and was needed "in order to conform with international standards of privacy protection and *to avoid possible barriers to trade*".[36] However, the Government was quick to observe that there were "few reported instances" of the misuse of personal data in the UK.[37] Ongoing scepticism about data protection was apparent in the White Paper. Equally, the view that the public sector was already subject to other safeguards was present in the document. For example, the White Paper noted that complaints against public sector data systems could be better investigated by ombudsmen.[38] This suggests that it was a more market approach, rather than an individual approach, that drove the Government's decision to legislate for both the public and private sectors in 1984.

The Government sought to adapt the Younger Committee Report in light of the 1981 Council of Europe Convention to produce "enforceable rules of law applying to both the private and public sectors."[39] At this point, although 11 states had signed the Convention, none had yet ratified it and the Convention itself had therefore not yet come into force, which was to follow ratification by 5 states.[40] The Government clearly anticipated that the 1981 Convention would be ratified. The 1982 White Paper expressly stated that registration requirements would extend to "central Government, local authorities, the police, nationalised industries

[33] Jay (2012), p. 10.
[34] See chapter 5, pp. 114 to 118.
[35] Home Office, Data Protection: The Government's Proposals for Legislation (April 1982) 1981/82 Cmnd. 8539.
[36] *Ibid.*, para. 2 (emphasis added).
[37] *Ibid.* (emphasis added).
[38] *Ibid.*, para. 21.
[39] *Ibid.*, para. 3.
[40] *Ibid.*, para. 5; 1981 Convention, Article 22(2).

and other public sector bodies",[41] subject to exemptions as permitted by derogations from the 1981 Convention, for the "purposes of national security", "the prevention and detection of crime" and in relation to "medical records" and "sensitive information recorded by social workers".[42]

The Data Protection Act 1984 was passed on 12 July 1984. It made provision for the application of a set of data protection principles[43] and established a Registrar and Tribunal[44] to oversee a scheme of registration and supervision of "data users" and "computer bureaux".[45] The "data users" and "computer bureaux" were defined in relation to data held or services provided in respect of data and therefore created no public-private divide.[46] The 1984 Act provided for individual rights to subject access,[47] compensation for inaccuracy,[48] compensation for loss or unauthorised disclosure,[49] and rectification and erasure.[50] Section 38(1) of the Act also stated that "a government department shall be subject to the same obligations and liabilities under this Act as a private person", save that a government department was not liable to prosecution under the Act,[51] although certain provisions would apply to civil servants directly.[52] In its core framework and definitions, therefore, the Act contained almost no public-private divide.

The 1984 Act did regulate data processing pursuant to statute with a lighter touch, reflecting state-facilitative derogations in keeping with the 1981 Convention. Data was obtained fairly "if it [was] obtained from a person who (a) is authorised by or under any enactment to supply it; or (b) is required to supply it by or under any enactment or by any convention or other instrument imposing an international obligation on the United Kingdom."[53] The Act also made exemptions the rights of data subjects "if the data consist of information which that person is required by or under any enactment to make available to the public, whether by publishing it, making it available for inspection or otherwise and whether gratuitously or on payment of a fee".[54] The Secretary of State had a power to exempt by order from the subject access

---

[41] Home Office, Data Protection: The Government's Proposals for Legislation (April 1982) 1981/82 Cmnd. 8539, para. 13.
[42] *Ibid.*, para. 17.
[43] Data Protection Act 1984, s. 2; Sch. 1.
[44] *Ibid.*, s. 3.
[45] *Ibid.*, ss. 4 to 12.
[46] *Ibid.*, ss. 1(5) and 1(6).
[47] *Ibid.*, s. 21.
[48] *Ibid.*, s. 22.
[49] *Ibid.*, s. 23.
[50] *Ibid.*, s. 24.
[51] Defined by s. 41 to include a Northern Ireland department and any body or authority exercising statutory functions on behalf of the Crown.
[52] Data Protection Act 1984, s. 38(2).
[53] *Ibid.*, Sch. 1(2).
[54] *Ibid.*, s. 30(1).

provisions where the disclosure of personal data was "prohibited or restricted by or under any enactment if he considers that the prohibition or restriction ought to prevail over those provisions in the interests of the data subject or of any other individual."[55] The Act also exempted personal data from the non-disclosure provisions "in any case in which the disclosure is… required by or under any enactment, by any rule of law or by the order of a court".[56] Statutory uses of data, therefore, enjoyed many advantages over private uses, reflecting the role of state-facilitative thought in the design of the legislation which sat alongside a broader market ambition.

The general provisions of the 1984 Act were also subject to a list of exemptions, many of which had special application to the public sector or state functions. This included exemptions for national security,[57] the prevention or detection of crime,[58] the apprehension or prosecution of offenders,[59] the assessment or collection of any tax or duty,[60] personal data held for the purpose of discharging statutory functions which had been obtained under the security or crime exemptions,[61] data held or acquired in the course of social work,[62] where subject access may prejudice the discharge of certain statutory functions relating to the regulation of financial and other services,[63] and certain information relating to judicial appointments.[64]

The 1984 Act did, however, contain a variety of other exemptions that addressed personal data consisting of information as to the physical or mental health of the data subject,[65] legal professional privilege,[66] payrolls and accounts,[67] personal, family or household affairs or information held only for recreational purposes,[68] backups,[69] preventing injury or other damage to the health of any person,[70] self-incrimination,[71] and examinations marks.[72] These served a variety of market and individual objectives, all sitting within the scheme of the 1981

---

[55] *Ibid.*, s. 34(2).
[56] *Ibid.*, s. 34(5).
[57] *Ibid.*, s. 27(1).
[58] *Ibid.*, s. 28(1)(a).
[59] *Ibid.*, s. 28(1)(b).
[60] *Ibid.*, s. 28(1)(c).
[61] *Ibid.*, s. 28(2)(a).
[62] *Ibid.*, s. 29(2).
[63] *Ibid.*, s. 30.
[64] *Ibid.*, s. 31(1).
[65] *Ibid.*, s. 29(1).
[66] *Ibid.*, s. 31.
[67] *Ibid.*, s. 32.
[68] *Ibid.*, s. 33.
[69] *Ibid.*, s. 34(4).
[70] *Ibid.*, s. 34(8).
[71] *Ibid.*, s. 34(9).
[72] *Ibid.*, s. 35.

Convention. This demonstrates the role of a variety of strands of approach which together gave full shape to the public-private divide.

Ultimately, the 1984 Act was therefore broadly reflective of a market-approach with state-facilitative exemptions following the pattern of the 1981 European Convention. National implementation of these obligations did not significantly challenge that approach, albeit that Government had voiced scepticism about the need for such legislation save where such legislation itself presented the risk of creating barriers to trade. In light of this scepticism, I suggest that the Government's implementation reflects an acceptance of the approaches developing in European data protection and little divergence through the agency of national actors, save state-facilitative exemptions as permitted by the 1981 Convention. European data protection was therefore an important influence and driver of national data protection law in 1984.

THE DATA PROTECTION ACT 1998

The Data Protection Act 1998 was introduced by the New Labour Government and then passed by Parliament on 16th July 1998.[73] The Act implemented the Data Protection Directive 1995. It reflected the broad market approach of that Directive. However, whereas the Directive showed heighted concern for individual rights, the Data Protection Act 1998 was arguably less onerous in several respects, reflecting a continuing and greater emphasis on a market approach, diverging from the European approach.

The implementation of the 1998 Act arguably reflected a more lenient approach to data protection than the 1995 Directive, reflecting a less individual and more market approach. This was the subject of an ongoing dispute between the UK Government and the European Commission, which considered infringement proceedings. This was on the basis that the Commission considered that the definition of 'filing system' in the 1998 Act was narrower than Article 2 DPD; the inclusion of 'recreational purposes' in the 1998 Act was broader than Article 3 DPD's household activities exemption; the 1998 Act treated criminal offences differently from other special categories of personal data; it exempted information required to be provided to data subjects under Articles 10 and 11 DPD; it made court remedies in regard to Article 12 DPD data subject rights discretionary; it exempted confidential references from the right to access under Article 13 DPD; it contained a narrower scope for non-material damage than Article 23 DPD required; the extent of monitoring assessments of international data transfer adequacy under Article 25 DPD was not satisfactory; and the

[73] Data Protection Act 1998, preamble.

investigative powers of the supervisory authority under Article 28 DPD were insufficient.[74] The Commission's complaint reflects the more market-friendly implementation of the Directive in the UK.

Similar to the Data Protection Act 1984, the 1998 Act contained key definitions based on the relationship of the actor to data rather than the public or private status of the actor. The 1998 Act used concepts of data controller, data processor and data subject, as in the 1995 Directive.[75] The data protection regime continued to grant rights to data subjects and others.[76] It continued to use a system of registration and notification.[77] The 1998 Act also contained an extended list of exemptions. Like the 1984 Act, many of these focussed on activity related to the public sector, including national security,[78] crime and taxation,[79] health, education and social work,[80] regulatory activity,[81] information available to the public by or under any enactment,[82] and disclosures required by law,[83] the armed forces, judicial appointments and honours, and Crown employment and Crown and Ministerial appointments.[84] To this extent, the endurance of a set of state-facilitative aspects is evident.

Equally, however, many exemptions under the Act protected other areas of activity, some of which concerned matters where disclosure could harm important aspects of commercial activity: journalism, literature and art,[85] research, history and statistics,[86] legal proceedings, legal advice and establishing or defending legal rights,[87] references, management forecasts, corporate finance, negotiations, examinations marks and scripts, and legal professional privilege.[88] The market logic inherent in many of these exemptions is apparent, permitting practices necessary for various activities to operate effectively.

The 1998 Act's enforcement provisions,[89] functions of the Commissioner,[90] an offence of unlawful obtaining of data,[91] and other provisions of the Act contained no aspect of a public-

---

[74] Letter of 16.12.2010 to Dr Chris Pounder from the European Commission in response to Complaint 3196/2007/(BEH)VL to the European Ombudsman.
[75] Data Protection Act 1998, s. 1.
[76] *Ibid.*, ss. 7 to 15.
[77] *Ibid.*, ss. 16 to 26.
[78] *Ibid.*, s. 28.
[79] *Ibid.*, s. 29.
[80] *Ibid.*, s. 30.
[81] *Ibid.*, s. 31.
[82] *Ibid.*, s. 34.
[83] *Ibid.*, s. 35(1).
[84] *Ibid.*, s. 37, Sch. 7. Recreational purposes were exempt under Data Protection Act 1998, s. 36.
[85] *Ibid.*, s. 32.
[86] *Ibid.*, s. 33.
[87] *Ibid.*, s. 35.
[88] *Ibid.*, s. 37, Sch. 7.
[89] *Ibid.*, ss. 40 to 50.
[90] *Ibid.*, ss. 51 to 54.
[91] *Ibid.*, s. 55.

private divide at the time the Act was passed. Some small differences existed, reflecting historic attitudes towards the liability of the Crown for criminal offences, as had been the case in the 1984 Act. Whereas corporate bodies could be liable of offences under the Act in certain circumstances,[92] the Act, in its application to the Crown, provided that

> Neither a government department nor a person who is a data controller by virtue of subsection (3) shall be liable to prosecution under this Act, but section 55 and paragraph 12 of Schedule 9 shall apply to a person in the service of the Crown as they apply to any other person.[93]

The first data protection principle required data processing to be fair and lawful.[94] Statutory authorisation or requirement would be sufficient to justify processing as fair.[95] The 1998 Act provided that data "are to be treated as obtained fairly if they consist of information obtained from a person who – (a) is authorised by or under any enactment to supply it, or (b) is required to supply it by or under any enactment or by any convention or other instrument imposing an international obligation on the United Kingdom."[96] To be fair, processing also had to meet a condition in Schedule 2 and, when processing sensitive personal data,[97] a condition in Schedule 3. Processing could satisfy Schedule 2 of the Act where it was necessary "(a) for the administration of justice, (b) for the exercise of any functions conferred on any person by or under any enactment, (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or (d) for the exercise of any other functions of a public nature exercised in the public interest by any person."[98] Schedule 3 7(1), which applied to sensitive personal data, was similarly satisfied where the processing was necessary "(a) for the administration of justice, (b) for the exercise of any functions conferred on any person by or under an enactment, or (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department." The breadth of this provision is such as to introduce a significantly more state-facilitative approach within the legislation, diverging from the approaches found in the Directive.

---

[92] *Ibid.*, s. 61.
[93] *Ibid.*, s. 63(5).
[94] *Ibid.*, Sch. 1, para. 1.
[95] *Ibid.*, Sch. 2, paras. 3 and 5.
[96] Data Protection Act 1998, Sch. 1, Part 2, para. 2(2).
[97] Sensitive personal data was defined as data consisting of information as to racial or ethnic origin, political opinions, religious beliefs or beliefs of a similar nature, trade union membership, physical or mental health or condition, sexual life, commission or alleged commission of any offence, or any criminal proceedings, the disposal of those proceedings or sentence in such proceedings: Data Protection Act 1998, s. 2.
[98] *Ibid.*, Sch. 2, para. 5.

The importance of this must be viewed against the ease with which public or private bodies could rely on their legitimate interests to process personal data fairly.[99] However, legitimate interests alone were insufficient for processing sensitive personal data.[100] Data processing pursuant to statutory functions or the functions of central government was therefore subject to less control than legitimate interest processing. This was state-facilitative in relation to sensitive personal data.

The 1998 Act, therefore, as initially passed, broadly reflected the European approach to the 1995 Directive, but took significant advantage of the opportunity to introduce state-facilitative exemptions. Although the implementation of the Directive was required by European law, we should not overlook the more market-friendly implementation of several provisions of the Directive in the Data Protection Act 1998. It therefore diverged from European law, driven by both market and state-facilitative approaches.

TRANSPARENCY AND THE PUBLIC SECTOR: STATE-RESTRICTIVE DEVELOPMENTS

As national data protection matured, even greater national divergence developed in the public-private divide. Governments, Parliament, and the courts all played a role in that process. The developments were not mandated by European data protection and reflect the role played by national actors and events, developing a more state-restrictive divergent approach in some areas.

FREEDOM OF INFORMATION AMENDMENTS TO THE DATA PROTECTION ACT 1998

The Freedom of Information Act 2000 and Freedom of Information (Scotland) Act 2002 made various amendments to the Data Protection Act 1998. The Freedom of Information Act 2000 was passed on 30th November 2000. In relation to public authorities only, the effect of these amendments was to broaden the right to subject access by analogy with FOIA rights and to create additional protections for the accuracy of personal data. These rights therefore became broader against such bodies than against the private sector. This was done to enhance transparency and accuracy, reflecting a limited extension of the state-restrictive approach to data protection.

Reforms in the Freedom of Information Act 2000 and Freedom of Information (Scotland) Act 2002 extended subject access request rights against public authorities, with similarities to Freedom of Information requests. It did this by expanding the definition of personal data to

---

[99] *Ibid.*, Sch. 2, para. 6.

[100] Sensitive personal data could only be processed fairly where a condition in Schedule 3 was met, in addition to a condition in Schedule 2: Data Protection Act 1998, Sch. 1, para. (1)(b). Schedule 3 did not contain any reference to legitimate interests and so an additional condition from the Schedule had to be met in the case of sensitive personal data.

include any "recorded information held by a public authority" which was not otherwise defined as personal data by section 1(1) of the Data Protection Act 1998.[101] The definitions of both "public authority" and "held" followed the definitions in the 2000 and 2002 Acts.[102] More information held by public authorities was therefore personal data than if the same information were held by private actors.

Where the additional personal data was "unstructured personal data", meaning it was not "recorded as part of, or with the intention that it should form part of, any set of information relating to individuals to the extent that the set is structured by reference to individuals or by reference to criteria relating to individuals",[103] a public authority was not required to comply with a subject access request unless the request contained a description of the data,[104] or if the estimated cost of compliance exceeded the limit set for FOI requests.[105] In this way, subject access requests regarding unstructured personal data mirrored FOI requests. The expansion of the subject access right against public authorities was driven by an approach that sought transparency from public authorities.

The expanded category of personal data was, however, exempt from all the data protection principles save the fourth principle (accurate and up to date) and sixth principle (the rights of data subjects but only to the extent of subject access rights and rights to rectification, blocking, erasure or destruction in cases of inaccuracy).[106] Rights to prevent processing likely to cause damage or distress, rights in relation to automated decision-taking, and rights to compensation, save where damage was caused by the violation of subject access rights or accuracy, were also exempted in relation to this personal data, as were notification requirements and the offence of unlawfully obtaining personal data.[107] In addition to transparency, the legislation therefore also enhanced legal protections of accuracy in the context of public authorities, although it did not extend other data protection rights. The reform was therefore a narrow extension of data protection, albeit reflecting a state-restrictive approach.

Limited categories of personal data held in purely unstructured manual format was exempted from the subject access and accuracy provisions. These categories comprised information related to "appointments or removals, pay, discipline, superannuation or other personnel

---

[101] *Ibid.*, s. 1(1)(e).
[102] *Ibid.*, s. 1(1) and s. 1(5). Note also that it did not apply to public authorities listed in Sch. 1 to the FOI Acts only in relation to information of a specified description, outside that description: see Data Protection Act 1998, s. 1(6).
[103] Data Protection Act 1998, s. 9A(1).
[104] *Ibid.*, s. 9A(2).
[105] *Ibid.*, ss. 9A(3) to (6).
[106] *Ibid.*, s. 33A(1).
[107] *Ibid.*

matters" in relation to service in the armed forces, in any Crown or public authority office or employment, or in an office, employment or contract for services where the power to take, determine or approve action in relation to appointments etc. was vested in the Crown, various Ministers or public authorities, was further exempt from all data protection principles and the rights of data subjects.[108] To this extent, a state-facilitative tendency can also be seen, tempering the expansion of data protection against public authorities in the Freedom of Information Acts.

The Freedom of Information Act 2000 also contributed to the development of a public-private divide in data protection in a second way. The Information Tribunal and national courts elaborated the definition of fair processing in the context of public authorities, where the processing entailed the disclosure of personal data pursuant to an FOI request. This jurisprudence recognised that for reasons of transparency in the public sector, a state-restrictive analysis, there were factors that make the disclosure of certain personal information held by public authorities about their senior officials and employees more likely to be fairly processed than similar processing in the private sector.

The Freedom of Information Act 2000 Act gave a general right of access to information held by public authorities.[109] This was subject to various exemptions. Of greatest importance for data protection was section 40(2). This provision conferred an exemption in relation to information that constituted personal data of individuals other than the FOI requester. It only applied where disclosure of such personal data to a member of the public would contravene "any of the data protection principles" or the right to prevent processing likely to cause damage or distress.[110] Section 40(2) conferred an absolute exemption in respect of disclosures that would breach the data protection principles, apparently removing any consideration of the public interest in disclosure.[111]

The first data protection principle, which included the requirement that processing must be "fair", therefore became important for determining whether a disclosure of personal data about officials was exempt from FOI requests. Subsequent case law therefore developed jurisprudence on fair processing in the context of public authority transparency obligations. In *Clift* v. *Slough Borough Council*, the court remarked that it was "a notable feature of the Directive and the DPA that they draw no distinction between public authorities and others".[112] However, the definition of fair processing was interpreted to make a distinction

---

[108] *Ibid.*, s. 33A(2).
[109] Freedom of Information Act 2000, s.1; ss. 3 to 6 define public authorities.
[110] *Ibid.*, s. 40(3).
[111] *Ibid.*, ss. 2(1) and 40(2).
[112] [2009] EWHC1550 (QB), para. 52.

based on the public or private context of certain processing. Section 40(2) FOIA has been the subject of a host of cases before the Information Tribunal.[113] Although the courts have noted that the fairness of processing is "justiciable… in terms of data protection… in the public as well as the private sector",[114] the public sector context has had an important impact on the assessment of what processing is fair. This reflects a further narrow extension of a state-restrictive approach.

In *Corporate Officer of the House of Commons* v *Information Commissioner*, the Tribunal considered whether the disclosure of MPs' travel expenses would be fair processing. The Tribunal considered that there were "three principal matters" that required resolution in relation to fair processing.[115] The third of these is most interesting for the purpose of the public-private divide: "Whether it is correct to draw a distinction between personal data related to an individual's public and his private life?".[116] The Tribunal accepted the ICO's proposed approach "which recognizes that in determining fair processing regard can be had as to whether the personal data relates to the private or public life of the data subject".[117] As the "public function is why the data is being processed" the Tribunal found that it could have regard to it.[118] The Tribunal held that "the consideration given to the interests of data subjects, who are public officials where data are processed for a public function, is *no longer first or paramount*"[119] and "where data subjects carry out public functions, hold elective office or spend public funds they must have the expectation that their public actions will be subject to greater scrutiny than would be the case in respect of their private lives".[120] The legitimate interests of the public included transparency and accountability in the use of public funds.[121]

---

[113] *A v Information Commissioner* EA 2006 0012, paras. 15 and 16; *Alcock v Information Commissioner* EA 2006 0022, paras. 29 to 33; *Corporate Officer of the House of Commons v Information Commissioner* 2007 WL 9362171; *London Borough of Bexley v Information Commissioner* EA 2006 0060; *MoD v Information Commissioner* EA 2006 0027; *London Borough of Camden v Information Commissioner* EA 2007 0021; *Guardian News and Media Ltd v Information Commissioner* EA 2008 0084; *Thackeray v Information Commissioner* EA 2009 0063; *Greenwood v Information Commissioner* EA 2010 0007; *Bousfield v Information Commissioner* EA 2009 0113; *Guardian Newspapers Ltd v Information Commissioner* EA 2010 0070; *Davis v Information Commissioner* EA 2010 0024; *Dun v Information Commissioner* EA 2010 0060; *Pycroft v Information Commissioner* EA 2010 0165; *T W Gibson v Information Commissioner* EA 2010 0165; *Trago Mills (South Devon) Ltd v Information Commissioner* EA 2012 0028; *Callus v Information Commissioner* EA 2013 0159; *Surrey Health Borough Council v Information Commissioner* [2014] UKUT 0339 (AAC).
[114] *Johnson v Medical Defence Union Ltd (No 2)* [2008] Bus LR 503, para. 47.
[115] Corporate Officer of the House of Commons v Information Commissioner 2007 WL 9362171, para. 74.
[116] *Ibid*
[117] *Ibid.*, para. 77; see also *Thackeray v. Information Commissioner* EA 2009 0063, para. 63.
[118] *Corporate Officer of the House of Commons v Information Commissioner* 2007 WL 9362171, para. 77.
[119] *Ibid.*, para. 78 (emphasis added).
[120] *Ibid.*
[121] *Ibid.*, para. 91.

Those "legitimate interests of members of the public outweighed the prejudice to the rights, freedoms and legitimate interests of MPs".[122] This is a state-restrictive analysis of the data protection rights of those who carry out public functions, hold office or are responsible for the expenditure of public funds.

Later Blake J in *Corporate Officer of the House of Commons v Information Commissioner*,[123] confirmed this approach and held that there was "no doubt that the public interest [was] at stake": the "expenditure of public money through the payment of MPs' salaries and allowances [was] a matter of direct and reasonable interest to taxpayers":

> In the end they bear on public confidence in the operation of our democratic system at its very pinnacle, the House of Commons itself. The nature of the legitimate public interest engaged by these applications is obvious.[124]

In *Ministry of Defence v Information Commissioner*, the Information Tribunal has also held that the expectations of civil servants differ from private employees because they "might be expected to lose some degree of anonymity on taking up such employment".[125] However, the jurisprudence did distinguish between senior and junior officials. In 2007 in *Department for Business, Enterprise and Regulatory Reform v Information Commissioner*,[126] the Information Tribunal addressed a Freedom of Information request for details of discussions between a government department and private lobbyists. The tribunal found that "a senior official of both the government department and lobbyist attending meetings and communicating with each other can have no expectation of privacy", whereas junior officials did have such an expectation.[127] In 2014 in *Edem v Information Commissioner*,[128] the claimant before the Court of Appeal was unable to make an argument that it was in his legitimate interests for the names of three junior employees of the Financial Services Authority, who had no responsibility for making "significant decisions", no "outward-facing role" and did not act as "spokesperson for the FSA", to be disclosed through a FOI request.[129] This narrow extension of the state-restrictive approach was therefore targeted at

---

[122] *Ibid.*, para. 93.
[123] [2008] EWHC 1084 (Admin).
[124] [2008] EWHC 1084 (Admin), para. 15.
[125] *MoD v. Information Commissioner* EA 2006 0027, para. 79.
[126] EA 2007 0072.
[127] *Ibid.*, para. 101.
[128] [2014] EWCA Civ 92.
[129] Ibid., paras. 3, 11 and 24. The reasoning is similar to that in C-28/08 *European Commission v Bavarian Lager* EU:C:2010:378 (29 June 2010), para. 78, in which the Grand Chamber of the ECJ found no "express and legitimate justification or any convincing argument" that the names of five junior officials should be disclosed in response to a request under similar provisions in Regulation (EC) No 1049/2001 of the European Parliament and of the Council of May 2001 regarding public access to European Parliament, Council and Commission documents.

senior officials, though this is of course consistent with a desire to subject decision-makers to greater scrutiny.

The effect of this court and tribunal jurisprudence was to introduce a public-private divide in relation to personal information held by public authorities. To the extent that the processing is rendered fair by the public context of the processing, it must be disclosed pursuant to an FOI request.[130] Private actors are not subject to FOI and, due to the absence of a public context, it is less likely that voluntary disclosure of employee personal data would be fair. The increase in transparency for public authorities under the 2000 Act has therefore contributed to the existence of this more state-restrictive feature in UK data protection law.

RESTORING TRUST IN PUBLIC SECTOR DATA: A STATE-RESTRICTIVE APPROACH FROM A STATE-FACILITATIVE OBJECTIVE

Reforms of the enforcement powers of the ICO also reflect a state-restrictive approach. However, this development in the public-private divide resulted from a complex interaction of state-restrictive and state-facilitative approaches. The Coroners and Justice Act 2009 amended the Data Protection Act 1998 to grant the ICO a power to issue assessment notices.[131] The power could only be used in relation to "(a) a government department, (b) a public authority designated for the purposes of this section by an order made by the Secretary of State, or (c) a person of a description designated for the purposes of this section by such an order."[132] Assessment notices permitted the ICO to carry out compulsory compliance assessments.[133] This reform followed in the wake of a 2008 data breach scandal involving data held by Her Majesty's Revenue and Customs (HMRC) and a number of other high profile data breaches in the public sector. In relation to provisions granting the ICO power to conduct compulsory audits of public authorities, Jack Straw MP, the Justice Secretary, said that the "Government recognise the need to strengthen the protection of personal data, and to restore public confidence in its security" following those breaches.[134] However, it would be misleading to consider the amendments brought about by the Coroners and Justice Act 2009 without considering the legislative history of the provisions and the other clauses that were ultimately withdrawn in the face of intense Parliamentary opposition. The Coroners and Justice Bill was not merely a state-restrictive set of provisions

---

[130] Given this, it would seem to follow that voluntary disclosure for the purposes of transparency is similarly fair processing.
[131] Data Protection Act 1998, ss. 41A to C. Unless of course another exemption applies independently.
[132] *Ibid.*, s. 41A (2).
[133] Data Protection Act 1998, ss. 52A to 52D were also added by the 209 Act and made provision for a data sharing code to be created by the ICO.
[134] H.C. Deb. 26 Jan 2009, vol. 487, cols. 42 to 43.

catalysed by serious failings in public sector data protection but part of a much broader executive agenda to encourage data sharing by public bodies: a state-facilitative ambition was, following Parliamentary resistance, reduced to state-restrictive provisions. In this case, therefore a struggle between state-facilitative and state-restrictive approaches shaped the public-private divide.

A consistent effort has been made by Government departments and public authorities in the UK to facilitate greater data sharing in the public sector within the framework provided by the Data Protection Act 1998.[135] The main way this has been attempted is through the expansion of statutory bases for the further processing of personal data. In this there is a deep vein of state-facilitative thought, although it has been constrained by a lively and sometimes vigilant state-restrictive tendency in UK politics.

THE CORONERS AND JUSTICE BILL 2009, CLAUSE 152

In 2007, HMRC suffered the largest personal data security breach in UK history, losing 25 million personal records. In November 2007, the Government consented to "spot checks" of government departments by the ICO.[136] By December 2007, the Government sought to increase the enforcement powers of the ICO to restore public trust. The ICO argued for "a power to inspect the processing of personal data without necessarily having the consent of the organisation concerned" and civil penalties for serious breaches.[137]

A key Government interest before the HMRC scandal was the development of a fast-track procedure to create more or broader legislative bases for data sharing.[138] The Government introduced proposed reforms to both enhance data protection and to improve data sharing in the Coroners and Justice Bill. The Secretary of State for Justice Jack Straw pointed to the recommendations of the Thomas Walport Review, which supported such reforms, and introduced clause 152 as a "new scheme for data sharing".[139] The scheme involved an extensive Henry VIII power to amend primary legislation. This power could be used to create

---

[135] Performance and Innovation Unit Report, Privacy and Data Sharing: The Way Forward for Public Services (2002); HM Government, Information Sharing Vision Statement (2006); HM Government, Transformational Government: Enabled by Technology, Annual Report 2006; Richard Thomas and Mark Walport, Data Sharing Review Report (2008).
[136] The Information Commissioner's Office Annual Report 2008-2009, p. 43.
[137] The Information Commissioner's Office Annual Report 2007-2008, p. 38.
[138] See Performance and Innovation Unit Report, Privacy and Data Sharing: The Way Forward for Public Services (2002), p. 13; Richard Thomas and Mark Walport, Data Sharing Review Report (2008), p. ii.
[139] H.C. Deb. 26 Jan 2009, vol. 487, col. 42. Richard Thomas was the Information Commissioner at this time.

powers to share information or remove statutory barriers to sharing in the public sector.[140] It received considerable opposition in Parliament, reflecting state-restrictive concerns.

The proposal attracted cross-party opposition. Shadow Attorney General Dominic Grieve criticised Straw for reducing "a seismic change in the relationship between the state and the citizen to something utterly benign" and the Government for "proposing to drive a coach and horse through the duty of confidentiality that the state owes to individuals in any case where a quite nebulous concept of public good decides to trump the private right".[141] Grieve labeled the proposal "draconian"[142] and argued that it raised "really serious possibilities of the oppressive state".[143] His opposition stemmed in part from concern about the Government's data security record.[144] David Howarth MP, the Liberal Democrat Shadow Secretary of State for Justice, criticized the proposals, saying they would "create amazingly broad exemptions to the principles of data protection legislation"[145] and voiced fears about the potential for the future abuse of such powers.[146]

Other fears were voiced about the level of parliamentary scrutiny orders under clauses 152 would receive[147] and the compatibility of the provision with Article 8 ECHR.[148] In the Public Bill Committee, evidence given by Liberty raised concerns that the legislation could "override all the protections contained in the Data Protection Act" and the Human Rights Act.[149] Liberty was also concerned about the broad scope of the power and lack of oversight and safeguards,[150] as well as the Government's record on data losses and security.[151] David Howard MP further critiqued the clause as "part of a bigger picture in which the state allows itself more and more powers to collect and process personal data about individuals for purposes that are not revealed to those individuals".[152]

Eventually, Bridget Prentice MP, Under-Secretary of State for Justice, offered to seek "a more streamlined version" of the clause with a greater role for Parliament so that "we will

---

[140] Coroners and Justice Bill, cl. 152.
[141] H.C. Deb. 26 Jan 2009, vol. 487, col. 42.
[142] *Ibid.*, col.43.
[143] *Ibid.*, col. 44.
[144] *Ibid.*, col. 51.
[145] *Ibid.*, col. 61.
[146] *Ibid.*, col. 62.
[147] *Ibid.*, col. 89.
[148] *Ibid.*, col. 110.
[149] Public Bill Committee Proceedings, Coroners and Justice Bill (H.C. 2008-2009 2nd Sitting) 3 February 2009, cols. 64 to 65.
[150] *Ibid.*
[151] *Ibid.*, col. 68.
[152]Public Bill Committee Proceedings, Coroners and Justice Bill (H.C. 2008-2009 9th Sitting) 26 February 2009, col. 356.

give the people whom we represent better public services."[153] The Government removed clause 152 during the Public Bill Committee stage on 10th March 2009.[154] Justifying that decision on 24th March 2009, Prentice said that the Government had "concluded that a more in-depth analysis of the features of an information-sharing power was needed".[155]

The enlarged enforcement powers of the ICO were therefore the residue of legislation intended to smooth the passage of the controversial clause 152. The public-private divide in the enforcement powers of the ICO was not in fact welcomed by the ICO and was repeated challenged in Parliament. Giving evidence to the Public Bill Committee, Richard Thomas argued for a "power to inspect without consent"[156] but commented that he was

> very concerned indeed that it extends only to Government Departments. Our report made it very clear that that sort of power is required right across the private and voluntary sectors for all data controllers.[157]

When questioned about the public-private divide, Thomas said

> we explicitly said that it no longer makes sense to draw sharp dividing lines between public, private and voluntary sectors. We have the use of private sector contractors, the involvement of the private sector in traditional public functions and the use of the voluntary sector to carry out public functions… It is right to have a global approach. We cannot draw those sorts of distinctions between the different sectors any more. That is one fundamental reason why we think the powers available to the commissioner's office need to extend to all data controllers.[158]

In the Public Bill Committee, David Howarth MP, in discussion of the clause, questioned its coverage of only the public sector.[159] His attempt to amend the provision to cover the private sector was later withdrawn.[160] He noted that "the power that holding vast amounts of data gives is not restricted to the public sector".[161] Additionally, he pointed out that "a lot of privatization of public services or at least contracting out of public services to either the

---

[153] *Ibid.*, col. 390.
[154] Public Bill Committee Proceedings, Coroners and Justice Bill (H.C. 2008-2009 15th Sitting) 10 March 2009, col. 586.
[155] H.C. Deb. 24 March 2009, vol. 490, col. 218.
[156] Public Bill Committee Proceedings, Coroners and Justice Bill (H.C. 2008-2009 4th Sitting) 5 February 2009, col. 133.
[157] *Ibid.*
[158] *Ibid.*, col. 135.
[159] Public Bill Committee Proceedings, Coroners and Justice Bill (H.C. 2008-2009 9th Sitting) 26 February 2009, col. 336.
[160] *Ibid.*, col. 352.
[161] *Ibid.*, col. 336.

private or voluntary sector" had blurred the lines between public authorities and private actors.[162] Labour MP Alun Michael voiced similar concerns,[163] arguing that "where a burden is needed in the public-interest to protect the public or individuals – it should apply fairly across the sectors".[164] He observed that

> At one time, an enormous amount of information would have been only in the public sector because it was gathered by or on behalf of authorities, or because the public sector undertook surveys and research, but that information is now very much part of the private sector's day to day activities.[165]

Similar concerns were raised by Conservative MP Henry Bellingham.[166] There was therefore cross-party opposition to the public-private divide in the ICO's enforcement powers. The ICO itself objected on the basis of an individual approach. On the other hand, the CBI opposed any change to the ICO's enforcement powers against the private sector,[167] including raising concerns about permitting search without a warrant.[168] The Government defended the remaining provision on a state-restrictive basis and resisted an individual approach.

Bridget Prentice MP replied that the "Government are strongly committed to improving public trust and confidence in the handling of personal information by public sector data controllers".[169] The proposed amendments represented "an unwarranted extension" of the ICO powers.[170] There was, in the Government's view, a "qualitative difference" between the public and private sectors:[171]

> Those who provide information to a data controller normally cannot refuse to do so, if they want to access a public service or have entitlement to a benefit. The public generally have no choice in that relationship, which is not exactly the same as that with the private sector.[172]
>
> …
>
> The fact that citizens must provide personal information to access essential services is a defining feature in the relationship between the citizen and the

---

[162] *Ibid.*, col. 337.
[163] *Ibid.*, col. 338.
[164] *Ibid.*, col. 339.
[165] *Ibid.*
[166] *Ibid.*, col. 341.
[167] *Ibid.*, col. 337.
[168] *Ibid.*, col. 342.
[169] *Ibid.*, col. 345.
[170] *Ibid.*, col. 346.
[171] *Ibid.*
[172] *Ibid.*

> public authority. In the private sector, the ability for someone to choose to go elsewhere should be a powerful driver that encourages businesses to look after personal information.[173]

This distinction between coercion in the public sector and choice in the private reflects a key aspect of state-restrictive thinking. Additionally, she argued on behalf of the Government that "additional burdens would be in conflict with the Hampton principles",[174] which sought to ensure that burdens on business were proportionate to the risk they sought to avoid. Assessments notices were a response to build public confidence after the HMRC breach[175] and would represent a "significant additional regulatory burden"[176] for business. Similar principles did not protect public authorities. Lord Bach, defending the Government's position in the House of Lords, argued that they were "an important step towards building public confidence in the handling of personal data by public-sector data controllers"[177] but would be a "little excessive and impose disproportionate burdens on business".[178] This appears to clearly reflect a state-restrictive thinking in which regulatory burdens on public authorities are viewed more positively. The Government was ultimately successful in passing assessment notices with a public-private divide in the face of this parliamentary opposition. In doing so, they introduced a public-private divide which is interesting in that it is state-restrictive, albeit that the provision was originally part of a wider state-facilitative intention. A struggle between different approaches of the Government and Parliament therefore shaped the public-private divide in this case, leaving a state-restrictive enforcement power in place.

ATTITUDE OF THE INFORMATION COMMISSIONER'S OFFICE TO THE PUBLIC-PRIVATE DIVIDE

The ICO has not adopted a public-private divide in its attitude to UK data protection. Instead it demonstrates elements of market and individual rights approaches. The introduction of public-private divides at the national level has been driven by Government, Parliament and the courts. None of the last three Information Commissioners have supported reforms or ideas that would introduce a public-private divide in national data protection law.

Although in an editorial for The Times in 2004, Richard Thomas stated that his "primary objective [was] preventing the emergence of a Big Brother Society",[179] his surveillance fears were not directed at an Orwellian state. Thomas argued that "data protection stops too much

---

[173] *Ibid.*
[174] *Ibid.*, col. 347.
[175] H.C. Deb. 24 March 2009, vol. 490, col. 218.
[176] *Ibid.*, col. 219.
[177] H.L. Deb. 21 July 2009, vol. 712, col. 1562.
[178] *Ibid.*, col. 1563.
[179] Times editorial, 14th August 2004, quoted in the Information Commissioner's Office Annual Report 2004-2005, p. 14.

information about our personal lives ending up in the hands of *governmental, commercial and voluntary organisations*". He was concerned to work against the establishment of a "surveillance society",[180] understood broadly. Indeed, the Thomas Walport Review, which he led with Mark Walport, sought to facilitate greater data sharing within government, subject to suitable safeguards.[181] Although Thomas's ICO addressed matters including ID cards, information sharing databases in children's services, the transfer of airline passenger details to foreign governments,[182] MPs' travel expenses,[183] the "Transformational Government" programme,[184] sharing personal information across the public sector,[185] and the "Connecting for Health" programme,[186] his focus was on the "danger of function creep",[187] "ensuring good practice"[188] and making sure there were proper "data protection safeguards"[189] in place. The fact that his ICO was consulted on many Government projects does not mean that the approach he brought to bear was a state-orientated one. For Thomas, building "trust and confidence" was "key" to data protection:[190] "mishandling personal information will lead to an erosion of confidence and *businesses and government* will suffer".[191] The Thomas ICO was the first body to voice serious concerns about the sale of personal information by private investigators in its 2006 special report "What Price Privacy?".[192] His concerns about surveillance spanned the public-private divide and reflect concerns for trust and confidence in the market and individual rights. Thomas's comments in his 2008-2009 Annual Report were indeed more state-restrictive in tone, noting the "need to limit the state's knowledge about the private lives of citizens", while increasing transparency about state activities.[193] However, he also consistently argued that Government proposals to empower the ICO to conduct compulsory audits was "seriously deficient" as it did not extent to the private sector.[194] The Thomas ICO's approach to data protection reform did not incorporated a public-private divide and on occasion explicitly rejected it.

---

[180] The Information Commissioner's Office Annual Report 2004-2005, p. 4 (emphasis added); see also The Information Commissioner's Office Annual Report 2005-2006, p. 6.
[181] Thomas Walport Report (2008).
[182] The Information Commissioner's Office Annual Report 2004-2005; The Information Commissioner's Office Annual Report 2005-2006, pp. 22 to 23; The Information Commissioner's Office Annual Report 2006-2007, p. 28.
[183] The Information Commissioner's Office Annual Report 2005-2006, p. 11
[184] *Ibid.*, p. 25.
[185] The Information Commissioner's Office Annual Report 2006-2007, p. 27
[186] *Ibid.*, p. 28.
[187] The Information Commissioner's Office Annual Report 2005-2006, p. 22.
[188] *Ibid.*, p. 23.
[189] The Information Commissioner's Office Annual Report 2006-2007, p. 28.
[190] The Information Commissioner's Office Annual Report 2005-2006, p. 3.
[191] *Ibid.* (emphasis added).
[192] Information Commissioners Office, What Price Privacy? (2006).
[193] The Information Commissioner's Office Annual Report 2008-2009, p. 11.
[194] *Ibid.*, pp. 13 and 42.

Christopher Graham's ICO used a less rhetorical style in its reports but continued to see its role as one of "upholding information rights in the public interest", irrespective of sector.[195] Although Graham was consulted and commented on the Protection of Freedoms Act, including restrictions on DNA profile retention, criminal vetting, the regulation of CCTV, restrictions on school biometric data use,[196] and was involved in consultations on reform of data sharing in the public sector,[197] his focus was on "enabling good practice"[198] across the public and private sectors rather than taking a state-restrictive or state-facilitative approach. Graham showed a more pragmatic approach to extending the ICO's assessment notice powers: where "it had become apparent that the case for the health sector was progressing faster" than that for local government, he supported the development, although he intended to seek further extension at a later date.[199] However, this was more reflective of a practical approach to extending the scope of a favoured regulatory tool rather than revealing any deeper shift in general approach. Graham saw the importance of "effective information rights" in "rebuilding necessary public confidence, both in digital services, *whether commercial or public sector*, and in transparent and accountable government".[200] He repeated calls for the extension of compulsory audit to the private sector[201] and his participation in the data sharing projects of the Cabinet Office and Law Commission balanced a recognition of the need for appropriate reforms with sufficient safeguards, within the scope of existing data protection law.[202] His approach therefore similarly reflected an individual approach.

Elizabeth Denham's speeches point to a trust and confidence approach without a public-private divide, rooted in tendencies characteristic of the market and individual approaches. In an early speech on 29 September 2016,[203] Denham emphasised that privacy and innovation go hand in hand, because a good privacy framework builds "foundations of trust" that are "integral" to innovation. Denham set out a "fundamental objective" to "build a culture of data confidence in the UK" with "greater trust in *businesses and public bodies*". Her vision was not of a "data protection regime that appeals because it is overly lax or 'flexible'" but one that

---

[195] The Information Commissioner's Office Annual Report 2011-2012, p. 8.
[196] *Ibid.*, p. 34.
[197] *Ibid.*, p. 38; The Information Commissioner's Office Annual Report 2012-2013, p. 18.
[198] The Information Commissioner's Office Annual Report 2012-2013, p. 8.
[199] *Ibid.*, p. 33.
[200] The Information Commissioner's Office Annual Report 2013-2014, p. 8 (emphasis added).
[201] *Ibid.*
[202] *Ibid.*, p. 31; The Information Commissioner's Office Annual Report 2014-2015, p. 32; The Information Commissioner's Office Annual Report 2015-2016, p. 27.

[203] Elizabeth Denham, *Transparency, Trust and Progressive Data Protection*, 29 September 2016, at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/09/transparency-trust-and-progressive-data-protection/.

“stands up to scrutiny”. Again, market and individual approaches are reflected in her views.

The ICO under the last three Information Commissioners has therefore not endorsed approaches that require a public-private divide. Rather, public-private divides have been developed by Government, Parliament and the courts, reflecting a mixture of state-restrictive and state-facilitative themes. However, the ICO had limited influence over UK legal developments in his regard.

THE PUBLIC-PRIVATE DIVIDE IN NATIONAL DATA PROTECTION

The development of the public-private divide in UK data protection law demonstrates complex interactions between the four conceptual approaches that have shaped the law in this area. Although market and individual approaches underpin the broad statutory scheme and the attitudes of successive regulators, Governments have been both more market-orientated than Europe and willing to countenance more state-facilitative approaches to data protection at the national level, albeit supporting apparently state-restrictive approaches where necessary to build the confidence necessary to support disclosure to the public sector. Freedom of Information has increased subject access and accuracy rights against public authorities and provided opportunities for the courts and tribunals to introduce state-restrictive tendencies in the jurisprudence on fair processing. Parliament has shown itself to be state-restrictive in the face of legislative attempts to increase data-sharing and in the passage of greater enforcement powers against the public sector for the ICO. One interesting phenomenon is the existence of provisions that, while state-restrictive in effect, were intended to help restore necessary public confidence to facilitate state activity and were intended as part of a package to smooth the passage of state-facilitative legislative bases for data sharing: state-restrictive in effect but state-facilitative in strategy. This is shows the complexities and nuances of the interaction of different approaches to the public-private divide. It does not show any linear or inevitable rise of an individual approach and also uncovers a history which is substantially more complex than that of a mere struggle, although struggle was also present in the development of the public-private divide in national data protection law.

CHAPTER 7

THE PUBLIC-PRIVATE DIVIDE AND UNAUTHORISED DISCLOSURE OFFENCES

INTRODUCTION

The criminalisation of the unauthorised disclosure of information by officials and government subcontractors is a significant feature of the public-private divide in UK individual information law. This chapter examines the development of the public-private divide in official secrecy and the large number of individual-identifying information disclosure offences in the UK, including those found in data protection law. This field has an intense focus on the state. Market and individual approaches have carried little weight, save in shaping minor data protection offences and a small number of other narrowly defined offences. It is an area that provides a clear counter example to claims which focus on a gradual shift towards a more pronounced individual approach to individual information. Instead, state-facilitative and state-restrictive approaches have come into conflict. To that extent it is one field that shows the role of struggle in the development of the public-private divide. Importantly, the chapter argues that the development of many unauthorised disclosure offences protecting individual-identifying information is not indicative of an individual approach but rather is usually state-facilitative in nature.

Official secrecy has dominated discussion in this field and reflects struggles between advocates of state-facilitative and state-restrictive approaches to the public-private divide. However, a focus on official secrecy alone would distract from an analysis of the existence of many unauthorised disclosure offences, the vast majority of which protect individual-identifying information. Although it is true that the emphasis on other disclosure offences intensified after 1989 in the aftermath of the reform of section 2 of the Official Secrets Act, disclosure offences existed independently before then. The criminal law has been used both to enhance the effectiveness of state activities and to restrain harmful disclosures of information acquired through the state's coercive power. The resultant legal framework is complex and inconsistent, reflecting ad hoc legislative developments. European institutions have had little influence over information law in this field. It is largely an area of national development. The influence of Europe across the development of the public-private divide in UK individual information law can therefore be seen to vary across confidentiality, the right to private life, data protection and the protection of individual-identifying information through the criminal law.

This chapter begins by examining the development of official secrecy. By the 1940s, a detailed legal regime had been created to regulate a wide range of official information.

Nothing of similar scope and strength has ever existed in relation to wrongful disclosure by private individuals.[1] It breadth was such as to cover individual-identifying information held by the state alongside a vast range of other information. The approach taken was distinctly state-facilitative. This is because it was designed to centralise control over disclosures by officials by the state, permitting authorised disclosures, backed by serious criminal sanctions for unauthorised disclosures. Although officials were criminalised, the intended effect was to strengthen the state's control over information, rather than to restrict the state from making disclosures at all.

The reform of the Official Secrets Acts in 1989 reflected the rise of a state-restrictive critique. This ultimately resulted in the narrowing of the scope of official secrecy in 1989. That retreat of the state-facilitative approach reflected concerns about the appropriate reach of the criminal law and was therefore state-restrictive, concerned that the state's powers to punish unauthorised disclosure were too great, in particular where disclosures were merely embarrassing, inconvenient or exposed the Government to criticism. It also reflected demands for greater transparency. However, the Official Secrets Act 1989 crystallised around several core areas of state concern: security and intelligence, defence, international relations and cooperation, and crime. The state-facilitative approach of the earlier law survived in relation to information disclosures that were likely to damage those central interests. The courts interpreted the 1989 Act to resist a more state-restrictive approach to official secrecy. The scope of official secrecy therefore reflects a tension between the state-facilitative approach favoured by the executive and the state-restrictive approach voiced by some Parliamentarians and civil society. These tensions continue to appear and are deeply ingrained. They illustrate well a dynamic of struggle as one of the complex interactions that can occur between the different approaches to the public-private divide. The recent Law Commission consultation on the Protection of Official Data reflects a continuation of a broader state-facilitative approach with concessions to state-restrictive elements. Civil society resistance was fiercely state-restrictive in response, criticising the Law Commission's closeness to Government Departments.

This chapter then considers other information disclosure offences. Data protection law has criminalised certain unauthorised disclosures of personal data since 1984 and does so without a public-private divide. However, these offences are best understood more as instances of a market approach rather than an individual approach because they enhance the control of data by data controllers rather than protecting the rights of data subjects. Importantly, they are subject only to fines and therefore the scope of other imprisonable

[1] See below, pp. 189 to 190.

offences are of greater importance to the public-private divide.[2] Many other information disclosure offences exist in the criminal law. A clear majority were passed after 1989. They reflect piecemeal attempts to respond to the narrowing of official secrecy, re-criminalising the unauthorised disclosure of information that would have fallen within section 2 of the Official Secrets Act 1911. Others, including those which existed before 1989, reflect a set of concerns about the disclosure of commercial or personal information acquired by the state in the exercise of its power. Although many of these offences protect information relating to businesses and individuals, thereby serving markets or personal privacy, they are best understood as more fundamentally state-facilitative or state-restrictive in ambition. In many cases, especially post-1989, the protection of commercial or personal information was motivated by state-facilitative considerations. Public authorities were granted legal control through the criminal law to help public authorities gather the information needed to perform their functions. The chapter takes the development of offences relating to taxpayer confidentiality as a case study to illustrate this point in greater detail. In a small number of other contexts, the criminalisation of unauthorised disclosure is intended to restrict public authorities from harming individuals and businesses, showing diversity of approach, especially through ad hoc state-restrictive provisions.

The development of official secrecy and other unauthorised disclosure offences highlights an area of individual information law which has consistently ignored or marginalised market and individual rationales and which shows a tension between state-facilitative and state-restrictive approaches. Although it sits comfortably with accounts that emphasise the struggle, at least regarding the state, it is a powerful counterexample for narratives that anticipate the rise of an individual approach. It shows the resurgence the state-restrictive approach in UK law but also the endurance of state-facilitative thinking.

OFFICIAL SECRECY: STATE-FACILITATIVE CONTROLS ON INFORMATION

The Official Secrets Acts 1911 to 1939 formed the most important and extensive part of the criminal law on unauthorised disclosure from 1948 to 1989. The Official Secrets Act 1911 was passed to replace the Official Secrets Act 1889,[3] in response to Government criticisms that it was ""full of weaknesses and difficult to operate". This perception made it unpopular with Governments.[4] In particular, the 1911 Act was intended to strengthen the hand of the state against the threat of espionage. Although the 1889 Act itself placed a great deal of power in the hands of the state to control official information, section 2 of the 1911 Act was

[2] *Ibid.*
[3] Official Secrets Act 1911, s. 13(2).
[4] Michael Everett, The Official Secrets Acts and Official Secrecy, House of Commons Library, Briefing Paper Number CBPO7422, 17 December 2015, p. 11.

incredibly broad, criminalising the unauthorised disclosure of all information obtained owing to official positions or entrusted in confidence by officials.[5]

The Official Secrets Act 1889 had been passed to maintain trust in government departments following a number of unauthorised disclosures before 1888.[6] The 1889 Act created offences of disclosure of information[7] and breach of official trust.[8] The offence of disclosure of information was an espionage offence, capable of being committed by any individual, official or private, who wilfully and without lawful authority communicated or attempted to communicate certain types of information "to any person to whom [the information] ought not, in the interests of the State, to be communicated at that time".[9] It criminalised communications of documents or knowledge obtained in contravention of the Act to those who "ought not, in the interests of the State" receive it at that time.[10] It also criminalised communications of certain information related to protected sites or naval or military affairs where the information had been "entrusted in confidence by some officer under Her Majesty the Queen".[11] It finally criminalised the wilful communication of certain documents or information relating to certain places belonging to the Crown, or relating to naval or military affairs, "to any person to whom he knows [it] ought not, in the interests of the State" be communicated.[12] The Act also criminalised breach of official trust.[13] Like later official secrecy legislation, the offence of breach of official trust in 1889 Act applied to state officials, official contractors and employees.[14] The personal scope of official secrecy legislation has remained substantially the same for nearly 130 years. The offence criminalised communications of certain documents or information "to any person to whom [it] ought not, in the interest of the State, or otherwise in the public interest" be communicated where the communication was corrupt or contrary to official duty.[15]

The 1911 Act was drafted to increase even further these considerable powers to apply criminal sanctions to officials. The circumstances of its passage through Parliament ensured little parliamentary scrutiny of the 1911 legislation. The catalyst for change was the "growing threat of international espionage"[16] in the context of the arms race preceding the First World

---

[5] Official Secrets Act 1911, s. 2(1)(a).
[6] Everett (2015), p. 10.
[7] Official Secrets Act 1889, s. 1.
[8] *Ibid.*, s. 2.
[9] *Ibid.*, s. 1(1)(b).
[10] *Ibid.*, s. 1(1)(b).
[11] *Ibid.*, s. 1(1)(c).
[12] *Ibid.*, s. 1(2).
[13] *Ibid.*, s. 2(1).
[14] *Ibid.*, s. 2.
[15] *Ibid.*, s. 2(1).
[16] Everett (2015), p. 6.

War.[17] This period was later described in Parliament as "the paranoia of 1911".[18] Lord Mishcon, during debates in the House of Lords on the Official Secrets Bill 1989, characterised the passage of the 1911 Act as one "passed in Parliament one afternoon in an atmosphere of some panic."[19] This context significantly strengthened the Government's hand, producing a state-facilitative Act of enormous breadth.

Viscount Haldane, Secretary of State for War in 1911, stated that the purpose of the Bill was to "strengthen the law" on official secrecy and espionage and to make it more effective.[20] The Government insisted that the Bill contained "nothing novel in the principle of the Bill" but that it was "desirable and necessary to remodel the legislation, in order to adapt it to particular circumstances or emergencies".[21] Many MPs complained about the speed with which the Act passed. The speed and lack of debate highlight the role of a powerful executive and relatively weak Parliament in the context of national security legislation. Those MPs who struggled to resist the Government's legislation were easily defeated. The motivation behind the 1911 reforms was strongly state-facilitative, aided by weak Parliamentary oversight and driven by military concerns.

Section 1 of the Act imposed penalties for spying. These could be committed by *any person* who did certain acts "for any purpose prejudicial to the safety or interests of the State",[22] which could be proved "if, from the circumstances of the case, or his conduct, or his known character as proved, it appears that his purpose was a purpose prejudicial to the safety or interests of the State".[23] Such acts could include obtaining or communicating information and it was therefore state-facilitative, in that it constrained the obtaining or communication of information to prejudice the state.

The most significant provision of the Act was section 2. It also criminalised the wrongful communication of information, extending this to information

- "which [related] to or [was] used in a prohibited place",
- "which [had] been made or obtained in contravention" of the Act,
- "which [had] been entrusted in confidence to him by any person holding office under His Majesty",
- or "which he [had] obtained owing to his position as a person who holds or has held office under His Majesty,

---

[17] *Ibid.*, p. 11.
[18] H.C. Deb. 21 December 1988, vol. 144, col. 483.
[19] H.L. Deb. 9 March 1989, vol. 504, col. 1610.
[20] H.L. Deb. 25 July 1911, vol. 9, col. 642.
[21] *Ibid.*, cols. 2252 to 2253.
[22] Official Secrets Act 1911, s. 1.
[23] *Ibid.*, s. 1(2).

- or as a person who holds or has held a contract made on behalf of his Majesty, or as a person who is or has been employed under a person who holds or has held such an office or contract".[24]

The 1911 Act, therefore, placed enormous power in the hands of the state to regulate the disclosure of official information. It covered all such information and criminalised disclosures without official authorisation. The 1911 Act also made it an offence to retain *certain* documents without a right to do so or when it was contrary to the person's duty.[25] Knowing receipt or receipt with reasonable ground to believe that the material or information was communicated in contravention of the Act was an offence, unless proved that the communication was contrary to the person's desire.[26]

It might be thought that the 1911 Act represented a high-water mark of a state-facilitative approach in the UK. However, the 1911 Act was subsequently strengthened by both the 1920 and 1939 Official Secrets Acts. The Official Secrets Act 1920 broadened the provisions of the 1911 Act to include the retention of *any* official document "for any purpose prejudicial to the safety or interests of the State" when it was "contrary to his duty to retain it" or one "fails to comply with any directions issued by the Government Department or any person authorised by such department with regard to the return or disposal" of the document.[27] It also made it an offence to permit others to have possession of official documents "issued for his use alone" or to communicate secret code words or passwords or to possess them where they had been issued to another person or, having obtained or found an official document, neglected or failed to restore it to the person or authority by whom or for whose use it was issued or to the police.[28] The 1920 Act also sought to make proof of offences more straightforward. It provided that communications with foreign agents *was evidence of* the commission of certain offences under the Official Secrets Acts.[29] The Official Secrets Act 1939 made further amendments relating to investigating offences under the Acts for the purpose of making prosecutions easier to obtain by creating powers to require the furnishing of information relating to official secrecy offences.[30]

This made the criminalisation of unauthorised disclosures made by official, government employees and government contractors incredibly broad. It was driven primarily by national security concerns and little scrutinised by Parliament. It imposed extensive and onerous

---

[24] *Ibid.*, s. 2(1).
[25] *Ibid.*, s. 2(1)(b).
[26] *Ibid.*, s. 2(2).
[27] Official Secrets Act 1920, s. 1(2)(a).
[28] *Ibid.*, s. 1(2)(b).
[29] Official Secrets Act 1920, s. 2.
[30] Official Secrecy Act 1939, s. 1.

obligations on official information. Nothing remotely comparable applied to information in private organisations. The approach reflects a very strong state-facilitative approach. It placed powerful tools in the hands of the state to regulate the flow of information held by its officials, employees and contractors, which were unavailable to private organisations.

The courts in the 1960s showed some tendency to uphold a state-facilitative approach to the Official Secrets Acts, influenced by concerns about justiciability, the separation of powers, and the reviewability of the royal prerogative in the courts. In *Chandler v DPP*, the defendants argued that a purpose to disrupt a nuclear airbase was not a purpose "prejudicial to the interests of the State" within the meaning of the Official Secrets Act 1911.[31] At the trial of the defendants, the judge had refused to allow the cross-examination of witnesses, and other evidence to be led, to challenge the defence policy of the Government. The defendants were members of the Campaign for Nuclear Disarmament. They sought to argue that their acts would in fact be beneficial to state interests, by inhibiting the state's ability to use nuclear weapons. They argued that the use of nuclear weapons would in fact have dire consequences for the state. The court held that the Crown was entitled to decide defence policy and that decision could not be called into question in a court of law. The interests of the state were therefore determined by the executive and evidence challenging that determination was not permitted. Although the case related to sabotage rather than the disclosure of information, this interpretation further strengthened the role of the state in determining the regulation of information within the state, by preventing juries from taking a different view of state interests. It was a state-facilitative driven by a deferential approach by the courts.

Lord Parker CJ held that once a "proposed act is ascertained… the only remaining question is whether that act is in fact prejudicial to the safety or interests of the State."[32] The defence policy of the state was an exercise of the royal prerogative and "the manner of the exercise of such prerogative powers cannot be inquired into by the courts".[33] Lord Reid did distinguish the state from the Government or executive but refused to interpret it broadly as "the individuals who inhabit these islands".[34] Instead he favoured "the country or the realm" or even "the organised community".[35] Although he refused to "subscribe to the view that the Government or a Minister must always or even as a general rule have the last word" about the public interest,[36] he considered that "the disposition and armament of the armed forces

[31] [1964] AC 763.
[32] *Ibid.*, p. 774.
[33] *Ibid.*, p. 775.
[34] *Ibid.*, p. 790.
[35] *Ibid.*
[36] *Ibid.*

are and for centuries have been within the *exclusive discretion* of the Crown and that no one can seek a legal remedy on the ground that such discretion has been wrongly exercised".[37] The "criminal system [was] not devised to deal with issues of that kind".[38] Viscount Radcliffe also considered that the matter was "not justiciable":[39] Lord Hodson similarly found the suggestion that a court could determine the interests of the state "an impossible proposition involving the court and jury in the consideration of questions of policy."[40] Lord Devlin said that "the statute is not concerned with what the interests of the State might be, or ought to be, but with what they actually are at the time of the alleged offence."[41] The statute protected "the objects of State policy, even though judged *sub specie aeternatis*, that policy may be wrong".[42] Although whether the purpose was prejudicial was a matter of fact for the jury, the definition of the "interests of the State" was for the Crown.[43] Lord Pearce similarly held that "interests of the State" did not mean "the interests of the amorphous populace":[44] "the interests of the State must… mean the interests of the State according to the policies laid down for it by its recognised organs or government and authority, the policies of the State as they are, not as they ought, in the opinion of the jury, to be."[45] The courts unwillingness to scrutinised the purported interests of the state and their deference to the executive in 1964 therefore reinforced the high degree of state-facilitative control over information in the Official Secrets Acts 1911 to 1939.

OFFICIAL SECRECY: THE RETREAT OF A STATE-FACILITATIVE APPROACH

Section 2 of the Official Secrets Act 1911 was widely criticised for being overly broad and for placing too much power in the hands of the executive to enforce secrecy through the criminal law. This resistance to the wide state-facilitative approach in the law led to the retreat of that approach. The 1972 Franks Committee argued for reform of section 2, proposing more limited categories of information, although accepting a role for conclusive ministerial certification of the appropriate classification of the information.[46] Although the Committee's recommendations were accepted in 1973 by the Conservative Government, no further action was taken at the time.[47] Under the Callaghan Labour Government, a 1978

---

[37] *Ibid.*, p. 791 (emphasis added).
[38] *Ibid.*
[39] *Ibid.*, pp. 797 and 798.
[40] *Ibid.*, pp. 800 to 801.
[41] *Ibid.*, p. 807.
[42] *Ibid.*, p. 808.
[43] *Ibid.*, p. 811.
[44] *Ibid.*, p. 813.
[45] *Ibid.*
[46] Stephanie Palmer, *In the Interests of the State: The Government's Proposals for Reforming Section 2 of the Official Secrets Act 1911* [1988] PL 523, 525.
[47] Everett (2015), p. 17.

White Paper and the 1979 Protection of Official Information Bill were proposed to implement this reform but it failed to attract sufficient support in Parliament before the 1979 General Election.[48] Such reforms would have limited the material scope of Official Secrets, although the executive would have maintained a large amount of ministerial control through the certification of classified information.

In 1989, the Government published a White Paper advocating reform of the 1911 Act. ATH Smith suggests that it was the Conservative Government's defeats in the Ponting trial in 1985[49] and the Spycatcher litigation, ending in 1988, that inspired legislative reform in 1989.[50] The same point was made by opponents of the Bill in Parliament.[51] Ponting had been prosecuted for leaking official documents about the sinking of the General Belgrano during the Falklands War. He was acquitted by the jury despite a direction from the trial judge that public interest disclosure was not a defence. The Spycatcher litigation sought unsuccessfully to prevent the publication of the memoirs of Peter Wright, a former MI5 officer. Both pieces of litigation resulted in considerable embarrassment to the Government and discredited so strong an approach to official secrecy. The 1989 White Paper proposed reform of the 1911 Act by narrowing the categories of information to which official secrecy applied, while maintaining a great deal of executive control in the areas in which official secrecy would continue to apply. It also proposed to enlarge the role of the jury in determining whether damage had in fact been caused to the relevant interest. There was therefore a retreat from the all-encompassing state-facilitative approach to official secrecy under the 1911 to 1939 Acts.

However, the proposed reforms maintained a state-facilitative approach to information whose disclosure could cause damage to certain state interests. The 1989 Act replaced section 2 of the 1911 Act with "provisions protecting more limited classes of official information",[52] narrowing official secrets but maintaining a focus on key areas of state concern. It protected six categories of information", namely, security and intelligence,[53] defence,[54] international relations,[55] crime and special investigation powers,[56] information resulting from unauthorised disclosures or entrusted in confidence,[57] and information

---

[48] Palmer [1988], p. 525.
[49] See Rosamund M Thomas, *The British Official Secrets Acts 1911-1939 and the Ponting Case* [1986] Criminal Law Review 491.
[50] ATH Smith, *Security Services, Leaks and the Public Interest* [2002] CLJ 514, 514.
[51] H.C. Deb. 21 December 1988, vol. 144, col. 489.
[52] Official Secrets Act 1989, preamble.
[53] *Ibid.*, s. 1.
[54] *Ibid.*, s. 2.
[55] *Ibid.*, s. 3.
[56] *Ibid.*, s. 4.
[57] *Ibid.*, s. 5.

entrusted in confidence to other states or international organisations.[58] The Act, while protecting the secrecy of such information, directs officials towards formal channels or authorised disclosure. Authorised disclosures by Crown servants or notified persons could be "made with lawful authority if, and only if, it is made in accordance with his official duty."[59] Authorised disclosures could be made by government contractors "if, and only if, it [was] made in accordance with an official authorisation or for the purposes of the functions by virtue of which he is a government contractor and without contravening an official restriction."[60] For other persons, authorised disclosures could be made "if, and only if, it is made to a Crown servant for the purposes of his functions as such or in accordance with an official authorisation".[61] A belief, with no reasonable cause to believe otherwise, that a person had lawful authority, was also made a defence.[62] This marked a retreat from, but not an abandonment of, the state-facilitative approach by the Government.

Opposition to the Bill centred around those who felt that the reforms should go further in introducing a more state-restrictive approach. There was a concern that secrecy made the executive too powerful and shielded it from accountability and potentially wrongdoing from exposure. There was therefore an ongoing tension between the state-facilitative core of official secrecy preserved by the Government and state-restrictive demands of opposition to the Bill. For example, Stephanie Palmer, commenting on the Government's reform proposals in 1988, criticised the proposed reform, arguing that "the government [had] its priorities wrong" because the "interests of political democracy demand maximum public access to official information" as a "safeguard against the abuse of power".[63] Palmer also criticised the proposed protection of all information about interception, fearing that in the absence of a public interest test it would permit illegal telephone tapping to be hidden. [64] Palmer was particularly critical of the absence of a public interest defence, arguing that "it is not always clear that it is in the public interest for information defined by the government as secret to remain so".[65] This was because past disclosures had in fact served the public interest.[66] She argued that the degree of executive control over information was "a dangerous situation for a political democracy"[67] as "excessive secrecy" allowed "governments to pursue their own

[58] *Ibid.*, s. 6.
[59] *Ibid.*, s. 7(1).
[60] *Ibid.*, s. 7(2).
[61] *Ibid.*, s. 7(3).
[62] *Ibid.*, s. 7(4).
[63] Palmer [1988], p. 524.
[64] *Ibid.*, p. 528.
[65] *Ibid.*, p. 531.
[66] *Ibid.*
[67] *Ibid.*

ends apart from the public interest", avoid scrutiny and "conceal mistakes and abuses".[68] Palmer's criticisms reflect a state-restrictive approach.

A similar vein of criticism was voiced by those who opposed the Bill in Parliament. Roy Hattersley MP, the Shadow Home Secretary and a prominent critic of the Bill, criticised the Government for failing to introduce greater freedom of information. He claimed that it continued the "cocoon of unnecessary and debilitating secrecy" around government.[69] He criticised the dominant role the Bill gave to the Government of the day in exercising control over information, arguing that Governments would inevitably fail to "distinguish between the true national interest and the sectional interests that they represent".[70] He feared that the Bill would prevent officials from exposing wrongdoing and merely serve the convenience of the Government.[71]

Others in Parliament emphasised the need for transparency both in government and for the sake of democracy.[72] They emphasised the importance of a public interest defence that would "enable crime, abuse of power and scandal to be exposed".[73] Tony Benn MP, an opponent of the Bill, argued that "if any structure of power is surrounded by secrecy, there is a danger of abuse".[74] Others were stronger in their criticism, accusing the Government of seeking to strengthen official secrets legislation to avoid embarrassment. For example, Diane Abbott MP claimed, with some hyperbole, that had the Government sought "ensure that all the people who had embarrassed the Government in the past would be caught by it and would serve time behind bars, this is the Bill that they would have come up with".[75] Abbott further criticised the Bill for conflating the public interest and the "interest of the Government of the day".[76]

Ultimately, this strong opposition, rooted in set of state-restrictive concerns, had little impact on the legislation. Several attempts to introduce public interest defences to the Bill were defeated.[77] The Government carried the necessary votes with comfortable majorities and built a regime around a state-facilitative approach, albeit one that more precisely targeted criminal sanctions around more limited classes of official information. The state-facilitative

---

[68] *Ibid.*, p. 535.
[69] H.C. Deb. 21 December 1988, vol. 144, col. 471.
[70] *Ibid.*
[71] *Ibid.*, cols. 476 to 478.
[72] Archer, *Ibid.*, col. 482; Robert Maclennan, *Ibid.*, col. 489; Tony Benn, *Ibid.*. cols. 504 to 505; Robin Corbett, *Ibid.*, col. 534, Lord Hatch of Lusby, H.L. Deb. 9 March 1989, vol. 504, col. 1636.
[73] Robert Maclennan, H.C. Deb. 21 December 1988, vol. 144, col. 492.
[74] H.C. Deb. 21 December 1988, vol. 144, col. 506.
[75] *Ibid.*, col. 518.
[76] *Ibid.*, col. 518.
[77] H.C. Deb. 22 February 1989, vol. 147, cols. 1036 to 1050; H.L. Deb. 03 April 1989, vol. 505, cols. 906 to 958.

approach might have retreated in the face of state-restrictive concerns but it was not defeated in core areas of state concern. The state-facilitative and state-restrictive approaches therefore interacted through tension, the state-restrictive making some gains through reform of section 2 of the 1911 Act but not fundamentally exposing official secrecy to the scrutiny of public interest disclosures.

The Home Secretary, Douglas Hurd MP, agreed that "the criminal law should be prised away from the great bulk of official information"[78] and only "protect, and protect effectively, information whose disclosure is likely to cause serious harm to the public interest.[79] The intention of the Bill was to more precisely and effectively target the criminal sanction in order to enhance and strengthen the ability of the state to control the flow of information in relation to key areas of state interest. However, it did not create freedom of information rights: internal discipline would still apply to breaches and there were no positive rights to disclosure.[80]

Importantly, the Bill made no provision for a public interest defence. It was based around a damage test, rather than a "serious harm" test as had been suggested in 1972 and by opponents of the Bill. Hurd argued that the definition of damage was for Parliament and not the courts,[81] that the harm test struck the appropriate balance of public interest, and that it was undesirable that "the court should be left to balance some sort of competing interest".[82] The Bill did, however, reflect a loosening of executive control to the extent that it rejected "the proposal for a ministerial certificate" in the Franks Report to instead rely on "objective criteria for the jury".[83] Hurd argued that secrecy was necessary for the effective protection of the nation by the Security Service.[84] Unauthorised disclosures by members or former members could endanger life and undermine the trust necessary for their work, which would

---

[78] H.C. Deb. 21 December 1988, vol. 144, col. 460.
[79] *Ibid.*, col. 460.
[80] Freedom of information rights were of course later created by the Freedom of Information Act 2000 (FOIA), which created a general right of access to information held by public authorities: FOIA, s. 1. Such disclosures are of course now authorised disclosures. However, the 2000 Act was drafted to avoid undermining the criminalisation of unauthorised disclosures offences. Information relating to national security, defence, international relations are all subject to exemptions: FOIA, ss. 24 to 27. However, these are not absolute exemptions and so are subject to a public interest test for disclosure: FOIA, s. 2. Importantly, there is an absolute exemption for information if its disclosure is "prohibited by or under any enactment": FOIA, ss. 44(1)(a) and 2(3)(h). This means that FOIA is excluded by the existence of any unauthorised disclosure offence and no public interest test is applied. Personal data is also subject to an absolute exception if disclosure would breach data protection principles: see FOIA, s. 40 and chapter 6, pp. 162 to 165.
[81] H.C. Deb. 21 December 1988, vol. 144, col. 465.
[82] *Ibid.*, col. 464.
[83] *Ibid.*
[84] *Ibid.*, col. 467.

"cause deep damage".[85] He also argued that there were "effective and reasonable ways for members of the security services and others affected to ensure that anxieties are not smothered and that concern about wrongdoing is not overlooked".[86] This reflected a state-facilitative approach in that strong criminal controls on disclosure were seen an encouraging officials to rely on formal internal mechanisms and authorised disclosure.

Supporters of the Bill also argued that internal controls were sufficient to prevent abuses of power. Jonathan Sayeed argued that "should they discover what they believe to be corruption or malpractice, they have not only the facility but the duty to report their concern to the permanent secretary, to the staff counsellor for the security and intelligence services, to the Minister or even to the head of the Civil Service."[87] Chris Patten argued that

> there is a place for a Crown servant with a worried conscience to go, but that place is not the front page of a newspaper or a surreptitious dispatch in a brown envelope. That is why we have a clear system of access to the head of the Civil Service and, in the case of members of the intelligence and security services, to the staff counsellor.[88]

Other supporters of the Bill argued that a public interest defence would "encourage leaks" after which "the harm has been done".[89] Lord Hunt of Tanworth feared that a public interest defence "would be a recipe for politicising the Civil Service" and damage the trust between Ministers and civil servants.[90] This reflected a state-facilitative concern to promote the working relationships of ministers and officials.

Attempts to introduce a public interest defence were later pursued unsuccessfully through the courts, which maintained the state-facilitative approach in the face of human rights challenge. In *R v Shayler*,[91] the defendant, a former member of the Security Service, had disclosed documents to a national newspaper purporting to reveal evidence of Security Service involvement in an assassination attempt against the head of government of a foreign State. The case concerned whether the Official Secrets Act 1989, read in light of the Human Rights Act 1998 and Article 10 ECHR, required a public interest defence. In the House of Lords,[92] the Court held that the 1989 Act could not be interpreted to contain a public interest defence. Lord Bingham held that the "natural and ordinary meaning and reading [of sections

---

[85] *Ibid.*
[86] *Ibid.*, col. 467.
[87] *Ibid.*, col. 502.
[88] *Ibid.*, cols. 540 to 541.
[89] Ivan Lawrence MP, H.C. Deb. 2 February 1989, vol. 146, cols. 519 to 535.
[90] H.L. Deb. 9 March 1989, vol. 504, cols 1616 to 1617.
[91] [2001] EWCA Crim 1977.
[92] *R v Shayler* [2002] UKHL 11

1(1)(a), 4(1) and 3(a)] in the context of the [Act] as a whole, was that a defendant prosecuted under these sections is not entitled to be acquitted if he shows that it was or that he believed that it was in the public or national interest to make the disclosure in question".[93] He added that the "sections leave no room for doubt" and that the "intention of Parliament [was] clear beyond argument."[94] However, this was not a violation of Article 10 because it was a ban on disclosure without lawful authority and a number of avenues were open to the defendant.[95] In this, the courts upheld the state-facilitative logic that drove the legislative majority to exclude a public interest defence on the face of the 1989 Act. The national courts have therefore done little to undermine the state-facilitative approach of the 1989 Act.

The continuing tensions between state-restrictive and state-facilitative approaches became apparent recently as the result of provisional conclusions drawn by the Law Commission of England and Wales in the course of its consultation paper on the protection of official data. The Law Commission consulted on reform of the official secrecy and wrongful disclosure offences in February 2017.[96] Its provisional conclusions reflect a broad continuation of the state-facilitative approach. These conclusions identified the definition of "enemy" under the 1911 Act as problematic because identifying another state as an enemy could have "negative diplomatic consequences"[97] and this could "inhibit the ability to prosecute".[98] The Law Commission acknowledged that the effect of changing the term would be "potentially to widen the scope of the offence"[99] but asked whether a broader definition of foreign powers might be "a helpful starting point".[100] The Law Commission also argued provisionally that it should no longer be necessary to "demonstrate actual prejudice"[101] to the interests of the state. Instead, it should be an offence "if the defendant, in intentionally engaging in the proscribed conduct, knew, or had reasonable grounds to believe that his or her conduct *may cause prejudice* to the safety or interests of the state".[102] It also provisionally concluded that it would be better "to focus on whether the defendant knew or believed that his conduct *might benefit* a foreign power."[103] This was because proving that the "defendant's conduct did in fact benefit foreign power could be very difficult given the nature of the activity in

---

[93] [2002] UKHL 11, para. 20.
[94] *Ibid.*
[95] *Ibid.*, para. 27.
[96] Law Commission, Protection of Official Data: A Consultation Paper (2017) Consultation Paper No 230.
[97] *Ibid.*, para. 2.110.
[98] *Ibid.*, para. 2.113.
[99] *Ibid.*, para. 2.114.
[100] *Ibid.*, para. 2.144.
[101] *Ibid.*, para. 2.135.
[102] *Ibid.*, para. 2.134 (emphasis added).
[103] *Ibid.*, para. 2.148 (emphasis added).

question."[104] The provisional conclusions regarding the 1911 Act all act to make it easier to prosecute individuals under that legislation and represent a strengthening of the state-facilitative approach. In relation to official secrecy, the provisional conclusions take issue with the requirement to prove damage or the likelihood of damage.[105] This is because such proof may have the "potential to compound the damage"[106] and the "requirement to prove the existence of a vulnerability" was an "obstacle" to prosecution.[107] The Law Commission suggested that a "inchoate mode" for the offence might be preferable.[108] This would require reason to believe in the capacity of the information to do damage. Notably, capacity is a lower bar than the likelihood of damage required under the 1989 legislation. The Law Commission also provisionally concluded that the notification process for making individuals subject to section 1(1) of the 1989 Act needed to be more efficient,[109] as "the process is slow… [and] sometimes a person must be notified at short notice".[110] The Law Commission also provisionally concluded that greater maximum sentences were required for breaches of official secrecy to "adequately reflect the culpability in the most egregious cases".[111] Finally, it provisionally concluded that "the problems associated with the introduction of a statutory public interest defence outweigh the benefits", although it did provisionally conclude that internal mechanisms should be improved.[112] In its efforts to make prosecutions easier and more efficient, to increase maximum sentences, and to reject a public interest defence the Law Commission's provisional conclusions represent a continuation and strengthening of a state-facilitative approach to official secrecy.

Media and civil society outrage following the publication of the consultation paper, on the other hand, reflect ongoing state-restrictive approaches in fierce conflict with the Law Commission's approach. In February 2017, significant concerns were voiced by journalists and civil liberties groups about some of the Law Commission's provisional conclusions and the potential impact of any reform on journalists and whistle blowers.[113] As a result, the

---

[104] *Ibid.*, para. 2.147.
[105] *Ibid.*, para. 3.137.
[106] *Ibid.*, para. 3.139.
[107] *Ibid.*, para. 3.143.
[108] *Ibid.*, para. 3.154.
[109] *Ibid.*, para. 3.178.
[110] *Ibid.*, para. 3.174.
[111] *Ibid.*, para. 3.186.
[112] *Ibid.*, para. 7.65.
[113] Evans, Cobain, Slawson, *Government Advisers Accused of 'Full-Frontal Attack' on Whistleblowers* (The Guardian, 12th February 2017): https://www.theguardian.com/uk-news/2017/feb/12/uk-government-accused-full-frontal-attack-prison-whistleblowers-media-journalists; Kjellsson and Mendick, *Journalists Who Obtain Leaked Official Material Could Be Sent to Prison Under New Proposals* (The Telegraph, 11th February 2017): http://www.telegraph.co.uk/news/2017/02/11/journalists-obtain-leaked-official-material-could-sent-prison/; *The Guardian View on Official Secrets: New Proposals Threaten Democracy* (The Guardian,

Government distanced itself from the project.[114] This fierce resistance by the media and civil society reflects a more state-restrictive approach, in which transparency, protection for whistle blowers and public interest disclosure defences act to prevent abuses of power by public authorities. The struggle between the state-facilitative and state-restrictive models of official secrecy is therefore very much ongoing.

UNAUTHORISED DISCLOSURE AND DATA PROTECTION

Unauthorised disclosure offences existed in both the Data Protection Act 1984 and Data Protection Act 1998.[115] These offences contain no public-private divide and have a very wide potential scope. The Data Protection Act 1984 made it an offence for a person, or their servant or agent,[116] "carrying on a computer bureau" to disclose connected personal data "without the prior authority of the person for whom those services are provided".[117] A "computer bureau" referred to one who provided "services in respect of data" as an agent who processed data on behalf of others or by allowing the use of equipment for processing data.[118] The concept was therefore very similar to a processor under the Data Protection Act 1998. Section 55 of the Data Protection Act 1998 made it an offence for a person to "obtain or disclose personal data or the information contained in personal data" or to "procure the disclosure to another person of the information contained in personal data" without the consent of the data controller, unless this was necessary "for the purpose of preventing or detecting crime" or was required by law,[119] there was a reasonable belief in the right to obtain, disclose or procure,[120] a reasonable belief that he would have had the consent of the data controller,[121] or that the act was justified in the public interest.[122] These offences were directed at preserving control over personal data in the hands of one who employed a

---

12th February 2017): https://www.theguardian.com/commentisfree/2017/feb/12/the-guardian-view-on-official-secrets-new-proposals-threaten-democracy; Chakrabarti, Whistleblowers *Keep Us Safe. We Can't Allow Them to Be Silenced* (13th February 2017): https://www.theguardian.com/commentisfree/2017/feb/13/whistleblowers-official-secrets-act-law-commission; Cobain, *This Assault on Whistleblowers Exceeds Even the Draconian 1911 Act* (The Guardian, 15th February 2017): https://www.theguardian.com/commentisfree/2017/feb/15/whistleblowers-law-commission-official-secrets-act.

[114] Bowcott and Mason, *No 10: Official Secrets Act Proposals 'Project of Previous Prime Minister'* (The Guardian, 13th February 2017): https://www.theguardian.com/law/2017/feb/13/uk-government-law-commission-report-outlaw-whistleblowers-investigative-journalism.

[115] There are also similar unauthorised disclosure offences in the Data Protection Act 2018, s.170, although this is out of the scope of the thesis. See chapter 1, p. 19.

[116] Data Protection Act 1984, s. 15(2).

[117] *Ibid.*, s. 15(1).

[118] Ibid., s. 1(6).

[119] Data Protection Act 1998, s. 55(2).

[120] *Ibid.*, s. 55(2)(b).

[121] *Ibid.*, s. 55(2)(c).

[122] *Ibid.*, s. 55(2)(d).

computer bureau or who was a data controller. The offences are not directed towards the rights of data subjects, as a data controller, for example, might consent to disclosures in violation of data subject rights. They serve the efficacy of the statutory scheme and the smooth running of computer bureau or data controller arrangements. They are therefore primarily reflective of a market approach, which operates as a broad baseline in this field.

However, the maximum penalty for an offence under section 15 of the Data Protection Act 1984 or section 55 of the Data Protection Act 1998 was a fine.[123] Although the Criminal Justice and Immigration Act 2008 provided for a power of the Secretary of State to amend section 55 by order to increase the maximum sentence to imprisonment of up to two years,[124] the power was never exercised and has now been repealed by the Data Protection Act 2018.[125] This means that the other offences considered in this chapter are typically subject to greater penalties, such as imprisonment, and transcend the market approach found in data protection, largely focusing on other approaches to the public private divide. The data protection offences are therefore of relatively minor significance.

Other Unauthorised Disclosure Offences in the Public Sector

A very large number of other offences of unauthorised disclosure have been created by statute. The Law Commission of England and Wales recently identified 124 such offences currently in force[126] and further offences have been passed since it published that research.[127] Most unauthorised disclosure offences apply only to certain individuals in the public sector, thereby creating a public-private divide in individual information law. They rely on authorisation and statutory powers for lawful disclosure. The offences usually demonstrate a state-facilitative approach in their extensive statutory authorisations or exemptions to disclose for the purposes of other statutory functions. It is important, in this context, to note that the majority of unauthorised disclosure offences were passed after 1989. Although the criminal law has never returned to the breadth and scope of the law as it was under section 2 of the Official Secrets Act 1911, reflecting state-restrictive concerns and greater scrutiny of criminal provisions, a state-facilitative approach has gradually eroded the impact of the reforms in the Official Secrets Act 1989. This shows the ongoing tensions between state-facilitative and state-restrictive approaches in the development of the law, albeit through gradual erosion rather than high-profile conflict. State-facilitative approaches

---

[123] Data Protection Act 1984, s. 19(2); Data Protection Act 1998, s. 60(2).
[124] Criminal Justice and Immigration Act 2008, s. 77. See Rosemary Jay, Data Protection Law and Practice (2012), paras. 21-32 to 21-38.
[125] The offence in the 2018 Act, s. 170 is also only subject to a fine: Data Protection Act 2018, s. 196(2).
[126] Law Commission (2017) Consultation Paper No 230.
[127] See, for example, the Digital Economy Act 2017.

have consistently and gradually undermined the reform of section 2 of the Official Secrets Act 1911.

Below, I analyse the criminalisation of disclosures related to taxpayer confidentiality in detail. It is also an important example due to the amount of information and number of officials covered by its provisions. This case study shows that even though offences related to taxpayer confidentiality, like many other offences, concern individual-identifying information, the core concern remains state-facilitative, rather than reflecting an individual approach. Criminalisation in the context of taxpayer confidentiality is also a key example of the expansion of criminal liability for wrongful disclosure by officials after the reform of section 2 of the Official Secrets Act 1911 in 1989. The scope of the criminal law expanded once again in 2005 as part of the merger of HM Inland Revenue and HM Customs and Excise, to support the significant advances in information sharing that those reforms brought about. Although the Commissioners for Revenue and Customs Act 2005 contained public interest disclosure provisions, these are a limited concession and do not undermine the state-facilitative framework, especially the public interest disclosure process is controlled by senior officials.

Many unauthorised disclosure offences do not simply protect all information gathered pursuant to the exercise of statutory power[128] or in the course of official duties, employment

[128] Atomic Energy Act 1946, s. 13; Coal Industry Nationalisation Act 1946, s. 56; Agricultural Marketing Act 1958, s. 47; Rivers (Prevention of Pollution) Act 1961, s. 12; Harbours Act 1964, s. 46; Medicines Act 1968, s. 118; Sea Fish Industry Act 1970, s. 14; Counter-Inflation Act 1973, Sch. 4; Employment Agencies Act 1973, s. 9(4); Health and Safety at Work Act 1974 etc., s. 33; Carriage of Goods (Prohibition of Discrimination) Regulations 1977/276, reg. 9(2); Highways Act 1980, s. 292(4); Fisheries Act 1981, s. 12; Public Passenger Vehicles Act 1981, s. 54; Civil Aviation Act 1982, s. 23; Industrial Training Act 1982, s. 6; Iron and Steel Act 1982, s. 33; Merchant Shipping (Liner Conferences Act 1982, s. 10; Telecommunications Act 1984, s. 101; Airports Act 1986, s. 74; Companies Act 1989, s. 86; Electricity Act 1989, s. 98; Water Act 1989, s. 174; Broadcasting Act 1990, s. 197; Child Support Act 1991, s. 50; Criminal Justice Act 1991, s. 91; Water Industry Act 1991, s. 206; Water Resources Act 1991, s. 204; Cardiff Bay Barrage Act 1993, s. 22; National Lottery Act 1993, s. 4C; Railways Act 1993, s. 145; Goods Vehicles (Licensing of Operators) Act 1995, s. 35; Shipping and Trading Interests (Protection) Act 1995, s. 3; Chemical Weapons Act 1996, s. 32; Airports (Groundhandling) Regulations 1997/2389, reg. 23; Bank of England Act 1998, Sch. 7; Data Protection Act 1998, s. 59; Landmines Act 1998, s. 19; Nuclear Safeguards Act 2000, s. 6; Television Licences (disclosure of Information) Act 2000, s. 3; Transport Act 2000, s. 143 and Schs. 9 and 10; Utilities Act 2000, s. 105; Communications Act 2003, s. 393; Public Audit (Wales) Act 2004, s. 54; Commissioners for Revenue and Customs Act 2005, s. 19; Education Act 2005, s. 109; Childcare Act 2006, s. 13B; Companies Act 2006, s. 460; National Health Service Act 2006, s. 8 and Sch. 22; Wireless Telegraphy Act 2006, s. 111; Statistics and Registration Service Act 2007, s. 39; UK Borders Act 2007, s. 42; Health and Social Care Act 2008, s. 76; Cluster Munitions (Prohibitions) Act 2010, s. 23; Postal Services Act 2011, s. 56; Civil Aviation Act 2012, Sch. 6; Customs Disclosure of Information and Miscellaneous Amendments Regulations 2012/1848, reg. 3; Legal Aid, Sentencing and Punishment of Offenders Act 2012, s. 33; Welfare Reform Act 2012, s. 129; Energy Act 2013, Sch. 9; Defence Reform Act 2014, Sch. 5.

or the administration of statutory schemes.[129] Instead, like taxpayer confidentiality, many protect individual-identifying information[130] or commercial information,[131] such as manufacturing processes, trade secrets and other information about businesses. This reflects a more targeted approach than the pre-1989 approach to official secrecy, but it often remains state-facilitative. This is because such offences facilitate centralised control over official information and facilitate the collection of information for official purposes by reassuring individuals and businesses that their information cannot be disclosed without proper authorisation. Unlike the 1989 Act, these offences do not require proof of the likelihood of damage to any particular interest.

Some exceptions to this remain, however, demonstrating the occasional impact of state-restrictive, individual or market approaches to the regulation of information through the criminal law, although these are relatively rare. Many powers of entry have unauthorised disclosure offences relating only to individual or commercial information indirectly acquired

[129] Rehabilitation of Offenders Act 1974, ss. 9 and 9A; Finance Act 1989, s. 182; Social Security Administration Act 1992, s. 123; Criminal Justice and Public Order Act 1994, s. 14; Criminal Appeal Act 1995, s. 23; Immigration and Asylum Act 1999, s. 158; Equality Act 2006, s. 6; Cross-border Railway Services (Working Time) Regulations 2008/1660, reg. 11; Crime and Courts Act 2013, s. 10; Mesothelioma Act 2014, s. 8; Criminal Justice and Courts Act 2015, Sch. 10, paras. 15 and 25.

[130] Rehabilitation of Offenders Act 1974, ss. 9 and 9A; Civil Aviation Act 1982, s. 23; Telecommunications Act 1984, s. 101; Electricity Act 1989, s. 89; Finance Act 1989, s. 182; Water Act 1989, s. 174; Child Support Act 1991, s. 50; Criminal Justice Act 1991, s. 91; Water Industry Act 1991, s. 206; Water Resources Act 1991, s. 204; Social Security Administration Act 1992, s. 123; National Lottery Act 1993, s. 4C; Criminal Justice and Public Order Act 1994, s. 14; Bank of England Act 1998, Sch. 7; Data Protection Act 1998, s. 59; Transport Act 2000, s. 143 and Schs. 9 and 10; Utilities Act 2000, s. 105; Commissioners for Revenue and Customs Act 2005, s. 19; Education Act 2005, s. 109; Childcare Act 2006, s. 13B; Companies Act 2006, s. 460; Statistics and Registration Service Act 2007, s. 39; UK Borders Act 2007, s. 42; Health and Social Care Act 2008, s. 76; Postal Services Act 2011, s. 56; Civil Aviation Act 2012, Sch. 6; Welfare Reform Act 2012, s. 129; Defence Reform Act 2014, Sch. 5; Mesothelioma Act 2014, s. 8; Criminal Justice and Courts Act 2015, Sch. 10, paras. 15 and 25.

[131] See Coal Industry Nationalisation Act 1946, s. 56(1); Industrial Organisation and Development Act 1947, s. 5; Statistics of Trade Act 1947, s. 9; Prevention of Damage by Pests Act 1949, s. 22(5); Medicines Act 1968, s. 118; Sea Fish Industry Act 1970, s. 14; Carriage of Goods (Prohibition of Discrimination) Regulations 1977/276, reg. 9(2); Highways Act 1980, s. 292(4); Fisheries Act 1981, s. 12; Public Passenger Vehicles Act 1981, s. 54; Industrial Training Act 1982, s. 6; Building Act 1984, s. 96; Telecommunications Act 1984, s. 101; Airports Act 1986, s. 74; Electricity Act 1989, s. 98; Water Act 1989, s. 174; Town and Country Planning Act 1990, ss. 196C and 325, Sch. 15(14); Water Industry Act 1991, s. 206; Water Resources Act 1991, s. 204; Water Resources Act 1991, s. 205; Cardiff Bay Barrage Act 1993, s. 22; Railways Act 1993, s. 145; Goods Vehicles (Licensing of Operators) Act 1995, s. 35; Chemical Weapons Act 1996, s. 32; Airports (Groundhandling) Regulations 1997/2389, reg. 23; Bank of England Act 1998, Sch. 7; Data Protection Act 1998, s. 59; Landmines Act 1998, s. 19; Nuclear Safeguards Act 2000, s. 6; Transport Act 2000, s. 143 and Schs. 9 and 10; Utilities Act 2000, s. 105; Communications Act 2003, s. 393; Companies Act 2006, s. 460; Wireless Telegraphy Act 2006, s. 111; Cluster Munitions (Prohibitions) Act 2010, s. 23; Postal Services Act 2011, s. 56; Civil Aviation Act 2012, Sch. 6; Defence Reform Act 2014, Sch. 5.

during their exercise.[132] The exercise of such powers does not require cooperation with the holders of that information and the information in question might be irrelevant to the purpose of the entry. Such powers are therefore state-restrictive in intention, protecting individuals and businesses from the indirect harmful effects of the exercise of state power. Some unauthorised disclosure offences are targeted at information that is dangerous or harmful information itself, in contexts which are not necessarily official.[133] Such offences reflect the occasional presence of an individual approach. This is because it is the potential harm to individuals, irrespective of the status of a potential disclosing party, that characterises the offence. Such offences apply to anyone who comes into possession of such information and are therefore broader in personal scope that the official secrecy related regime. Others, such as the Access to Information (Post Commencement Adoptions) (Wales) Regulations 2005/2689, regulation 19 and the Access to Information (Post Commencement Adoptions) Regulations 2005/888, regulation 21, apply to all providers of a service, whether public or not, in this case registered adoption societies. Such offences reflect a recognition of service provision across the public-private divide. Some offences relate to the wrongful disclosure of business information in a commercial setting. These offences reflect market approaches and are not limited to officials or focused on individual-identifying information, although some such information may be included within the scope of commercial information.[134] Individual and market approaches underlie such disclosure offences. This demonstrates the variety of approaches that occasionally influence the passage of ad hoc unauthorised disclosure offences. They are however more unusual examples compared to state-facilitative offences. The majority of offences cover official information that was formerly covered by section 2 of the Official Secrets Act 1911. They act to restore control over that information for state-facilitative ends. A clear example of this is in relation to taxpayer confidentiality.

TAXPAYER CONFIDENTIALITY

For much of the 20th century, secrecy in relation to taxpayer information was enforced through the criminal law in the Official Secrets Acts and through internal disciplinary proceedings.[135] Solemn declarations of secrecy by tax officials were much older and have

---

[132] Prevention of Damage by Pests Act 1949, s. 22(5); Gas Act 1965, s. 9; Building Act 1984, s. 96; Town and Country Planning Act 1990, ss. 196C and 325, Sch. 15(14); Water Resources Act 1991, s. 205; Private Security Industry Act 2001, s. 19.

[133] Atomic Energy Act 1946 (certain information about atomic energy plants); Anti-Terrorism, Crime and Security Act 2001, ss. 79 (information that might prejudice the security of any nuclear site or of any nuclear material) and 80 (information about the enrichment of uranium or any information or thing which is, or is likely to be, used in connection with the enrichment of uranium).

[134] Companies Act 1985, s. 449; Companies Act 1989, s. 86.

[135] Osita Mba, *Transparency and Accountability of Tax Administration in the UK: The Nature and Scope of Taxpayer Confidentiality* (2012) British Tax Review 187, 207.

been imposed since the Income Tax Act 1799.[136] Secrecy at that time supported the introduction of a system of self-assessment by reducing opposition to the tax's onerous and intrusive disclosure requirements.[137] Mba states that "it is arguable that the primary rationale for tax secrecy was not the protection of privacy of taxpayers *per se* but the facilitation of the imposition and collection of income tax."[138] Customs and excise officers were not required to make similar declarations.[139] This reflected the reduced practical rationale for the state protecting confidentiality outside the context of self-assessment. Customs and excise officers relied to a much greater extent on intelligence gathering and search and seizure powers, which do not require, or indeed presuppose, the cooperation of taxpayers. This reflected their historic role in tackling smuggling activities.

There has been consistent and long-standing recognition of the role of taxpayer confidentiality in facilitating the collection of tax. In *Inland Revenue Commissioners v National Federation of Self-Employed and Small Businesses Ltd*, Lord Wilberforce observed that the "total confidentiality of assessments and of negotiations between individuals and the revenue is a vital element in the working of the system."[140] More recently, the Permanent Secretary for Tax told Parliament in 2011 that "if taxpayers believe that their information may be disclosed, it will make it very much more difficult for us to collect tax".[141] In 2014, the HMRC Tax Assurance Commissioner told MPs that there was "'extremely overwhelming' evidence that ending taxpayer confidentiality would result in a loss of tax revenue":[142]

> The reason we don't have to use our powers extensively is that the public have confidence in us, and the taxpaying public is willing to share information, and sometimes more information than they are required [to share].[143]

In response to an oral question in March 2016 calling for greater transparency, Lord Ashton of Hyde explained that:

> My Lords, taxpayer confidentiality is key to the effective operation of the tax system. Taxpayers have confidence that the sensitive information that they give to HMRC will be protected and this trust underpins the high levels of

---

[136] *Ibid.*, p. 189.
[137] *Ibid.*, pp. 204 to 205.
[138] *Ibid.*, p. 205.
[139] *Ibid.*, p. 206.
[140] *Inland Revenue Commissioners v National Federation of Self-Employed and Small Businesses Ltd* [1982] AC 617, 633.
[141] Andrew Goodall, Taxpayer confidentiality: Harnett sets out HMRC view for MPs, Tax Journal, 21 October 2011.
[142] Andrew Goodall, MPs ask HMRC to justify taxpayer confidentiality, 14th October 2014, http://www.accountingweb.co.uk/tax/hmrc-policy/mps-ask-hmrc-to-justify-taxpayer-confidentiality.
[143] *Ibid.*

> voluntary tax compliance that the UK enjoys. The public benefit of taxpayer confidentiality lies in the overall effectiveness of the tax administration that it significantly supports.

The policy behind preserving taxpayer confidentiality is therefore not the protection of individuals but rather the facilitation of the collection of tax by the state, which requires individual-identifying information from taxpayers. Taxpayer confidentiality also illustrates the way in which such state-facilitative individual information disclosure offences are part of a wider, if ad hoc, erosion of the reform of section 2 of the Official Secrets Act 1911. Although individual privacy certainly benefits from taxpayer confidentiality, it would be mistaken to consider that these offences are directed primarily at protecting the individual or restricting the state. It is rather a necessary part of the assurances given to support the maximum tax yield and to encourage voluntary disclosure, which is more efficient than coerced disclosure. Taxpayer confidentiality is therefore a state-facilitative practice.

The argument above can be substantiated through a more detailed historical consideration of interventions made during the enactment of the Official Secrets Act 1989 and policy changes which followed. In 1989, a number of MPs voiced concern that the removal of a criminal sanction for the unauthorised disclosure of taxpayer information would damage the collection of tax. Concerns for taxpayer confidentiality were also voiced in the House of Lords, as were hopes that the matter would be addressed in the Finance Bill of the same year.[144] The value of taxpayer confidentiality was once again stressed in terms of the effective operation of the tax system.[145] Chris Patten MP, the Minister for Oversees Development, announced during debates on reform of the Official Secrets Acts that separate criminal provision would be made to protect taxpayer confidentiality,[146] although it would be targeted at information about taxpayers, including companies, and exclude information about tax policy and administration.[147] Patten also noted at that time that other areas might need further criminal legislation in the future. This would be considered on a Bill by Bill basis.[148] Lord Belstead finally confirmed in the House of Lords that the Government's intention was to make provision in the Finance Bill to protect taxpayer confidentiality through the criminal law.[149]

---

[144] Lord Houghton of Sowerby, H.L. Deb. 9 March 1989, vol. 504, col. 1619.
[145] *Ibid.*, col. 1621.
[146] H.C. Deb 22 February 1989, vol. 147, cols. 1073.
[147] *Ibid.*
[148] *Ibid.*, cols. 1074.
[149] H.L. Deb. 09 March 1989, vol. 504, col. 1665.

Section 182 of the Finance Act 1989 was introduced to protect taxpayer information following the narrowing of Official Secrets legislation in that year.[150] The section came into force on the *same day* as the repeal of section 2 of the Official Secrets Act 1911.[151] Taxpayer confidentiality was therefore never without the protection of the criminal law. Unlike official secrets legislation, section 182 and later protections have focussed on "identifiable persons" and not all information relating to tax. However, it would be wrong to argue that this represents a shift towards an individual approach. The reason for this is that taxpayer confidentiality, rather than official secrecy generally, was and is understood to play an important role in ensuring the effective collection of tax. Denying confidentiality to taxpayers was seen as threatening the tax base and it is this, rather than a concern for individual interests and values, that has driven the protection of taxpayer confidentiality in the UK. It is best understood as a targeted criminal offence designed to facilitate the state rather than to protect individual interests. This also explains its application to tax officials and not more generally to those wrongfully disclosing the same information, such as, for example, private accountants.

Section 182(1) made it an offence for a person to disclose "any information which he holds or has held in the exercise of tax functions… if it is information about any matter relevant, for the purposes of those functions, to tax or duty in the case of any identifiable person". Section 182(4) made it an offence for a person to disclose

> any information which he holds or has held in the exercise of functions of the Comptroller and Auditor General and any member of the staff of the National Audit Office, or of the Parliamentary Commissioner or Administration and his officers, is, or is derived from, information which was held by any person in the exercise of tax functions and is information about any matter relevant, for the purposes of tax functions, to tax or duty in the case of *any identifiable person*.[152]

These offences do not apply to disclosure with lawful authority, consent of the individual identified, or "which has been lawfully made available to the public before the disclosure is made."[153] Belief in lawful authority, without cause to believe otherwise, is a defence.[154] The section was successively amended to extend to tax credit functions,[155] child trust fund

[150] Mba (2012), p. 208.
[151] Finance Act 1989, s. 182(12).
[152] Emphasis added.
[153] Finance Act 1989, s. 182(5).
[154] *Ibid.*, s. 182(7).
[155] By the Tax Credits Act 1999, s. 12(2)(a).

functions,[156] certain social security functions[157] and other audit and Ombudsmen functions.[158] Although an expanding scope of the offence to new functions was adopted by the state over time, the same rationale subsisted.

Offences protecting taxpayer confidentiality were further expanded to facilitate extensive data sharing on the merger of Inland Revenue and Excise and Custom to form HMRC in 2005. The O'Donnell Review was announced in July 2003 to consider the organisations responsible for tax policy and administration.[159] The O'Donnell Review sought "a coherent approach to information"[160] in order to use "information provided by taxpayers to develop a better understanding of customer needs so that policies and services can be best targeted".[161] With other organisational reforms, the aim was "to improve efficiency in the revenue departments".[162] The O'Donnell Review led to the Commissioners for Revenue and Customs Act 2005, the main purpose of which was to merge Inland Revenue and Excise and Customs to form HMRC.[163]

The Commissioners for Revenue and Customs Bill was introduced by the Paymaster General Dawn Primarolo MP on 24thNovember 2004. At the Bill's Second Reading, she said the Bill was "principally a machinery-of-Government Bill to implement sensible reforms to tax administration", including reforms to the use of information.[164] The Bill would make "better use of information, built around an ability to look across a taxpayer's affairs" to "allow for more effective targeting of resources to areas of risk".[165] This would include allowing HMRC "to pool information internally so that information supplied for one of its functions can be used for any of its other functions".[166] She promised that there would be "no let-up in HMRC's commitment to safeguarding taxpayer confidentiality".[167] The Bill extended the protection of the criminal law to many matters previously dealt with by Customs and

---

[156] By the Child Trust Funds Act 2004, s. 18(2)(a).
[157] By the Social Security Contributions (Transfer of Functions, etc.) Act 1999, Sch. 6 para. 9(2)(a).
[158] By the Government of Wales Act 1998, Sch.12 para. 31(2); Budget Responsibility and National Audit Act 2011, Sch. 5(2) paras. 14(2)(a) and 14(2)(b); Public Audit (Wales) Act 2013, Sch. 4 para. 2; Public Services Ombudsman (Wales) Act 2005, Sch. 6 para. 22(a), Scottish Public Services Ombudsman Act 202 (Consequential Provisions and Modifications) Order 2004/1823, art. 10(b).
[159] Gus O'Donnell, Financing Britain's Future: Review of the Revenue Departments (2004), para. 1.1.
[160] *Ibid.*, para. 1.20.
[161] *Ibid.*, para. 1.33.
[162] *Ibid.*, para. 1.34.
[163] Commissioners for Revenue and Customs Bill, Bill 3 of 2004-05, Research Paper 04/90, 6 December 2004, p. 10.
[164] H.C. Deb. 8 December 2004, vol. 428. cols. 1147 to 1170.
[165] *Ibid.*, col. 1170.
[166] *Ibid.*, col. 1174.
[167] *Ibid.*

Exercise.[168] Dawn Primarolo justified this extension of the criminal law by reference to the needs of tax administration:

> It is vital for continuing compliance rates that taxpayers provide information to the Revenue departments. The bedrock of that process is the knowledge that their confidentiality is protected.[169]

Andrew Tyrie MP echoed such concerns: "If people do not have confidence in the Revenue department, they will not share information and the tax yield will suffer."[170] David Heathcoat-Amory MP added that taxpayer confidentiality was "important, and it is very much in the interests of the Revenue departments, because people will co-operate freely with the Revenue authorities only if they can be sure that the information given is protected".[171]

The Commissioners for Revenue and Customs Act 2005 merged Inland Revenue and Customs and Excise into HMRC. Section 17(1) facilitated an enormous pooling of information held by the Commissioners of Inland Revenue and the Commissioners of Customs and Excise, "their staff and anyone acting on their behalf".[172] It provided that "information acquired by the Revenue and Customs in connection with a function may be used by them in connection with *any other function*", subject to any restrictions in statute or international agreements.[173] A significant feature of the merger was this enormous expansion of the use of information for any function of HMRC. Section 18 provided that "Revenue and Customs officials may not disclose information which is held by the Revenue and Customs in connection with a function of Revenue and Customs",[174] unless it is a disclosure which was made in one of a list of statutorily recognised circumstances.[175] The section 18 duty of confidentiality was backed by an offence of wrongful disclosure in section 19. Section 19(1) provided that a "person commits an offence if he contravenes [the confidentiality duties imposed by the Act] by disclosing revenue and customs information relating to a person whose identity is specified in the disclosure or can be deduced from it."[176] There was a defence of reasonable belief that the disclosure was lawful or that it "had already and lawfully been made available to the public".[177] The Commissioners for Revenue and Customs Act 2005 also imposed an obligation on "each person who is appointed under

---

[168] *Ibid.*
[169] *Ibid.*, col. 1175.
[170] *Ibid.*, col. 1186.
[171] Public Bill Committee, Commissioners for Revenue and Customs Bill (H.C. 2004-2005 2nd Sitting) 11 January 2005, col. 58.
[172] Commissioners for Revenue and Customs Act 2005, s. 17(3).
[173] *Ibid.*, s. 17(2) (emphasis added).
[174] *Ibid.*, s. 18(1).
[175] *Ibid.*, ss. 18(2) and (3).
[176] *Ibid.*, s. 19(1).
[177] *Ibid.*, s. 19(3).

this Act as a Commissioner or officer of Revenue and Customs" to make a "declaration acknowledging his obligation of confidentiality under section 18",[178] "as soon as is reasonably practicable following the person's appointment".[179]

Unlike the Official Secrets Acts, the 2005 Act contained provision for public interest disclosures. However, it remains tightly controlled and subject to oversight by the Commissioners for Revenue and Customs. It is therefore a provision more in line with a state-facilitative approach: placing control in the hands of the organisation as to whether information is released in the public interest, which is defined so as to cover core areas of state concern, including the prevention of crime;[180] the regulation of professional misconduct concerning HMRC's functions;[181] police functions concerning the free movement of persons or goods;[182] and public safety and public health.[183] Section 20 could be relied on where a disclosure is "made on the instructions of the Commissioners (which may be general or specific)",[184] is of a certain class,[185] and "the Commissioners are satisfied that it is in the public interest."[186] It is emphatically not a public interest defence of the kind favoured by the opponents of the Official Secrets Act 1989, which would protect decisions made without official agreement. Further disclosure without the consent of the Commissioners is not permitted and may be punished under section 19.[187]

The expansion of offences concerning taxpayer confidentiality illustrates a process of the gradual erosion of the reform of section 2 in pursuit of state-facilitative aims by a major unauthorised disclosure offence. A state-facilitative approach has therefore eroded the retreat of section 2 of the Official Secrets Act 1911 without the open conflict that characterised the legislative struggle in 1989.

Struggles Over the Criminalisation of Unauthorised Disclosure

Official secrecy and other unauthorised disclosure offences have maintained a strong public-private divide, using the criminal law to control information disclosure by officials, government employees and contractors. Although the scope of the criminal law on official secrecy has narrowed and been more precisely targeted towards a core set of state concerns, it has largely followed a state-facilitative approach, with a state-restrictive

---

[178] *Ibid.*, s. 3(1).
[179] *Ibid.*, s. 3(2A).
[180] *Ibid.*, s. 20(2).
[181] *Ibid.*, s. 20(3).
[182] *Ibid.*, s. 20(4).
[183] *Ibid.*, s. 20(6).
[184] *Ibid.*, s. 20(1)(a).
[185] *Ibid.*, s. 20(1)(b).
[186] *Ibid.*, s. 20(1)(c).
[187] *Ibid.*, s. 20(9).

approach unsuccessfully opposing changes pushed through Parliament by a powerful executive. Reform was driven by a desire to refine the state-facilitative approach and to respond to broader concerns about over-criminalisation, at best reflecting a retreat in the face of state-restrictive criticisms. That retreat has been subsequently eroded by many targeted wrongful disclosure offences in the public sector. The national courts have also largely supported a state-facilitative approach to official secrecy, although very few decisions have arisen for judgment.

Official secrecy and other unauthorised disclosure offences are a key example of the dominance of a state-facilitative approach in an area of individual information law. It reflects features of the UK constitutional landscape, especially executive dominance of Parliament and the unwillingness of the courts to intervene in core areas of state power. It also reflects the limited role of European information law on the development of national criminal law. The scope of the state-facilitative approach was significantly eroded by state-restrictive critiques in the 1970s and 1980s and expanded in a piecemeal fashion thereafter through unauthorised disclosure offences. It reflects struggles between state-facilitative and state-restrictive approaches with limited consideration for individual or market approaches. The criminalisation of unauthorised disclosure has been highly resistant to expansion into disclosures of information held by private actors, producing only relatively minor data protection offences. It is an important counter example to narratives of a gradual rise of the individual approach in information law. Although admittedly it does demonstrate the role of struggle, the gradual expansion of a state-facilitative approach through unauthorised disclosure offences after 1989 is a different form of interaction between those approaches. The development of the public-private divide in the criminal law on unauthorised disclosure shows the complex ways in which the approaches can interact, in this field predominantly through competition and struggle.

CHAPTER 8

THE HISTORY OF THE PUBLIC-PRIVATE DIVIDE IN UK INDIVIDUAL INFORMATION LAW: COMPLEX INTERACTIONS BETWEEN DIVERSE APPROACHES

INTRODUCTION

The history of the public-private divide in UK individual information law does not support either of the two distinctive historical narratives about the development of the public-private divide identified in chapter 1.[1] It does not reflect a general, paradigmatic shift from a state-restrictive and towards an individual approach. Neither does it support historical accounts that emphasise the importance of struggle as the main form of interaction between different approaches to the development of individual information law. Instead, the thesis provides a historically-grounded theoretical model for understanding the set of complex interactions between diverse approaches that shaped the public-private divide in individual information law between 1948 and 2017. The adoption of market, individual, state-restrictive or state-facilitative approaches by a variety of executive, legislative, judicial and regulatory actors and the tensions, compromises, cooperation, inspiration, catalysation, reaction, resistance, erosion, evolution, parallel coexistence and shifts in approach between those approaches explain the uneven and non-linear development of the public-private divide better than rival theories. The thesis provides a more complex and nuanced account for thinking about the development of the public-private divide and the sets of concerns, attitudes, assumptions and tendencies that have shaped it.

The thesis also contributes to the "ontological challenge" in the Europeanisation literature. It does this by helping to illustrate the complex, inconsistent and diverse ways in which UK individual information law at the national level has implemented, resisted, or diverged from European individual information law concerning the public-private divide. It shows the agency of national actors interacting with European law and the role of the approaches that span the division of national and European law. It also helps to illustrate that the influence of Europe has been uneven in respect to different fields of individual information law: more influential in relation to data protection and human rights and less influential in relation to pre-Human Rights Act confidentiality and unauthorised disclosure offences. The historical approach adopted demonstrates the complex interactions of approach that have framed the decisions of architects of that divide. Those interactions implicate a variety of actors across time, in various locations and different levels of governance. The thesis identifies that those interactions are subject to trends, ebbs and flows in importance. European developments

[1] See chapter 1, p. 6.

have, at various points, been adopted, accommodated, engaged with, or resisted at the national level.

The thesis is also important because the historically-grounded theoretical framework it provides is able to inform the broader scholarship on the public-private divide in individual information law. Our historical narratives matter. The narrative of a paradigmatic shift from a state-restrictive to an individual approach is liable to create important blind spots, especially a failure to account for enduring or resurging approaches that treat public authorities distinctively. Similarly, the narrative of struggle risks obscuring the role played by diverse interactions between different approaches, especially the complex relationship between market and individual approaches in the development of European data protection law.[2]

The wide-ranging analysis found in this thesis is needed because a wide range of areas of law impact on the public-private divide in individual information law. The thesis helps to show why a more holistic view is necessary. A narrow focus on reforms to the public-private divide in privacy or data protection law risk being undermined by developments in confidentiality or statutory controls in national law, especially in relation to disclosure by public authorities. Theorists who oppose the public-private divide in information law concerned with individuals need to look beyond privacy and data protection to appreciate the broader legal landscape and therefore the likely effect of reforms to remove the public-private divide. For example, loosening state-restrictive legality requirements on some public authorities in human rights or data protection jurisprudence would be readily undercut by the approach to confidentiality in *Ingenious Media*.[3] Efforts to encourage public authorities to innovate with data on a par with the private sector and embrace the advantages of new technologies can be threatened by risk aversion linked to the proliferation of statutory offences.[4]

The thesis highlights the importance of engagement with the theories and arguments that underpin the different approaches identified in this thesis as the public-private divide in individual information law develops in the future. In particular, the thesis highlights priorities for scrutiny and justification or reform. Public authorities receive distinctive treatment in relation to their duties of confidence;[5] the common law fundamental right to *Marcel* confidentiality;[6] the Article 8 ECHR requirement of standards of legal precision, detail, foreseeability and accessibility of public authorities, with substantive safeguards and

[2] See chapter 5.
[3] See chapter 2, pp. 48 to 51.
[4] See Law Commission, Data Sharing between Public Bodies (2014) Law Com No. 351, p. 77.
[5] See chapter 2, pp. 39 to 47.
[6] See chapter 2, pp. 48 to 51.

effective controls, that are not required of private actors;[7] the imposition of controls on public authorities not placed on private actors by the Human Rights Act 1998;[8] the GDPR's imposition of various state-restrictive requirements on public authorities, and in particular its denial of reliance on "legitimate interest" processing;[9] the heightened transparency, accuracy and oversight requirements in national data protection;[10] the criminalisation of various unauthorised disclosures of individual-identifying information held by public authorities;[11] and abounding state-facilitative exemptions.[12] A satisfactory theory of information law must reconcile this distinctiveness with the literatures on privacy and data protection that generally reject public-private divides. It requires a better understanding of why public authorities might require distinctive treatment, either state-facilitative or state-restrictive. There is therefore a need to situate this distinctiveness within a broader constitutional theory regarding individual information, its limits and its interaction with markets and civil society and to successfully integrate the positive insights of each approach while identifying their proper limits.

The thesis identifies the role of historical choices that are bound up with our current arrangements.[13] By providing a richer and more detailed history of the public-private divide in information law and presenting a complex picture of its development, it has the potential to inform understanding and reflection on the diverse normative underpinnings of the public-private divide in individual information law.[14] This is relevant for thinking about whether the law should be reformed. For example, this thesis shows the role of the Single Market and European harmonisation in the development of the public-private divide according to a market approach. Now that European data protection no longer relies on Article 100a EC and has its own legal basis in Article 16 TFEU, there is a question of whether should it nevertheless preserve all or part of the historically market approach. Where the historical choices bound up in current arrangements are the result of European integration, and to the extent that Brexit might ultimately change the nature of that connection, there will be new questions about whether the approaches bound up in the GDPR should be preserved or the new potential for reform realised. This will require a careful consideration of normative considerations embedded in its historical development and illuminated by the thesis.

Although the scholarship on the changing nature and structure of the state makes plausible the expectation that the public-private divide would have diminished over time, the history of

---

[7] See chapter 3, pp. 73 to 76, and chapter 4, pp. 87 to 95.
[8] See chapter 4, 80 to 96.
[9] See chapter 5, pp. 133 to 144.
[10] See chapter 6, pp. 160 to 170.
[11] See chapter 7, pp. 190 to 198.
[12] See p. 216.
[13] See John Allison, *History in the Law of the Constitution* (2007) 28 Journal of Legal History 263.
[14] See chapter 1, pp. 8 to 10.

the public-private divide suggests that no strong connection exists between these changes and the development of the law.[15] There is a need to account for the continued appeal of the different approaches. The intertwining of public authorities and private actors, related demands for intrusive information practices, public authority regulatory and commissioning roles, the use of technology and transfer of information across the public-private divide and within mixed bureaucracies has not had unilateral or monolithic effects on the development of the public-private divide.[16] Changes in approach to the public-private divide reflect complex interactions between different approaches to the public-private divide. There is a need for deeper consideration of the reasons for the persistence of these approaches and the values that inform them. The thesis also shows that the existence and interaction of the different approaches is a point of continuity within an area characterised by scholarship on the information society, which emphasises expectations of revolutionary change. It resists historical determinism and points to a more complex reality.[17]

EUROPEANISATION AND THE PUBLIC-PRIVATE DIVIDE

Europe has acted to inspire, catalyse and require change in UK information law at various points in the history of the public-private divide.[18] National divergence, resistance and reluctance to change in response to European pressure all form part of the history of this divide. This forms an important contribution to the "ontological challenge" of Europeanisation literature: how to explain asymmetries across settings in processes of legal change in Europe.[19] The literature sets ongoing agency and choice against various deterministic claims. It emphasises that legal development is often non-linear, fragmented, and shaped by agency and choice in response to "the pressures emanating directly or indirectly from [Europe]".[20] The thesis contributes to such literature, by clarifying "the role of structure and agency within the Europeanization process" and "identifying the mechanisms that are the interactive link between the "domestic" and the "EU" spheres of activity".[21] In common with that literature, the thesis highlights that Europeanisation is a "complex reality" with elements of both convergence and fragmentation,[22] with "differential or asymmetrical impact[s]".[23] This

---

[15] See chapter 1, p. 9.
[16] See chapter 1, pp. 10 to 13.
[17] See chapter 1, pp. 13 to 16.
[18] See chapter 1, pp. 19 to 21.
[19] Kevin Featherstone, "Introduction: In the Name of Europe", in Kevin Featherstone and Claudio Radaelli (eds.), The Politics of Europeanization (2003), p. 13.
[20] *Ibid.*, p. 7.
[21] *Ibid.*, p. 13.
[22] Kevin Featherstone and Claudio Radaelli, "A Conversant Research Agenda", in Featherstone and Radaelli (eds.) (2003), p. 340.
[23] *Ibid.*, p. 338.

can be seen in the complex interactions of diverse approaches by various European and national actors during the development of the public-private divide.

The thesis finds common ground with claims that the "impact of Europeanisation is typically incremental, irregular, and uneven over time and between locations, national and subnational".[24] With it, the thesis has illustrated asymmetries[25] of "absorption, accommodation, and transformation"[26] and "acknowledges the dynamism, imbroglio, and limits to determinism in present-day Europe".[27] This can be seen across European and national human rights, European and national data protection, confidentiality, and official secrecy and unauthorised disclosure offences.

As Higgs has noted, regarding the development of the information state in UK, its "long, complex and discontinuous process" requires a "more interesting history of information".[28] The thesis provides an important part of that history and a historically-grounded theoretical framework for understanding its development. The history of the public-private divide demonstrates that although, as Wincott rightly says, Europe is a dynamic forum "built through political contexts and struggles",[29] the public-private divide is not the fruit of struggle alone. This thesis does not point to the "ubiquity of struggle" in which "patterns of past struggle [are] woven into the fabric of stability".[30] A richer set of interactions characterises legal development in this field and have woven themselves into the law.

THE APPROACHES OF VARIOUS ACTORS TO THE PUBLIC-PRIVATE DIVIDE

The development of the public-private divide has not involved a straightforward shift from one paradigm to another. Nor is it merely the product of struggle. Instead, the thesis demonstrates the complex ways in which proponents of different approaches have interacted to shape the architecture of information law. Struggle is only one form of interaction found in this development. There was also compromise, cooperation, inspiration, catalysation, reaction, resistance, erosion, evolution, parallel coexistence and shift in emphasis or approach over time. No one approach has dominated consistently over time. No one approach can accurately be described as outdated or anachronistic, at least in the

---

[24] Featherstone, "Introduction: In the Name of Europe", in Featherstone and Radaelli (2003), p. 4.
[25] *Ibid.*, p. 18.
[26] *Ibid.*, p. 19.
[27] *Ibid.*
[28] Edward Higgs, The Information State in England: The Central Collection of Information Since 1500 (2003), p. 11.
[29] Claudio Radelli, "The Europeanization of Public Policy". in Featherstone and Radelli (eds.) (2003), p. 13.
[30] David Kennedy, A World of Struggle: How Power, Law and Expertise Shape Global Political Economy (2016), p. 7.

sense that all four approaches continue to play an active role in shaping the public-private divide.

National Governments have often acted, both at the national and European level, to pursue a state-facilitative approach in relation to the public sector. Market approaches have also found favour with Governments. Parliament has often, dominated by the executive, supported the Government of the day, although parliamentarians have also resisted some stronger state-facilitative tendencies successfully and remain a voice for state-restrictive concerns. The Blair Labour Government was unusual in supporting the passage of the Human Rights Act 1998 and Freedom of Information Act 2000, both of which, partly through jurisprudential development by the courts and certainly as drafted, contributed to the resurgence of the state-restrictive approach in the UK. This should not be exaggerated, however, as New Labour showed itself to be state-facilitative in various ways, especially in the attempt to pass broad statutory information sharing powers.[31]

In UK individual information law, Government remains a powerful actor. Often able to dominate Parliament and thereby able to make use of its sovereignty, executive architects of the public-private divide have considerable influence. One tendency is to use this power to protect key public authorities from law that might inhibit or undermine their ability to perform their functions. A state-facilitative approach is therefore likely to result where the executive is developing policy and have an interest in protecting the public sector. Parliament is often a forum for dissent but more rarely makes that dissent felt. The national courts have moved beyond support for a market approach and a state-facilitative attitude to public authorities towards support to an individual approach and some more state-restrictive tendencies. Courts have been influential in shaping the common law and developing jurisprudence in relation to legislative regimes. They have not felt bound to replicate the approaches which influenced legislators, either in Europe or at the national level. Though Europe has been very important in the development of human rights and data protection, national courts, Governments and Parliament have all shown themselves willing to take divergent approaches to the public-private divide at times. Within the Europeanisation literature some structural accounts emphasise the role of "structural convergence".[32] By contrast, this thesis highlights the important role of different approaches to the public-private divide which do not always mirror structural expectations.[33]

---

[31] See chapter 6, pp. 165 to 170.
[32] Tanja Borzel, "Conceptualising the Domestic Impact of Europe", in Featherstone and Radaelli (eds.) (2003), p. 66.
[33] Christopher May, The Informational Society: A Sceptical View (2002), pp. 13 to 14.

European and national regulators have frequently supported individual or market approaches. Sometimes the market approach has been instrumentalised to further an agenda more interested in the individual approach. The European Commission and Parliament have always supported market approaches but have increasingly come to support an individual approach. Data protection as a fundamental right is in the ascendancy in Europe. It is not clear whether Article 8 CFR will diverge from Article 8 ECHR regarding tensions between the state-restrictive and individual approaches. The European courts demonstrate ongoing tensions between state-restrictive and individual approaches to the public-private divide, showing the influence of each in their jurisprudence.

CONFIDENTIALITY

The history of the law of confidence in the UK shows little influence of struggle nor a gradual shift from a state-restrictive towards an individual approach. It has been developed almost exclusively by the national courts, at least until the development of the tort of misuse of private information, and so illustrates an area of development that was not significantly shaped by Europe, at least until the Human Rights Act 1998. The jurisprudence is not best described as revealing conflict or struggle. Rather, over the course of its development, the national jurisprudence has been influenced and shaped by shifting emphases of approach by the courts and the parallel coexistence of different approaches within different lines of case law. These shifts are little acknowledged, let alone best framed as struggle. All four approaches feature. The recent resurgence of the state-restrictive approach undermines the claim that the individual approach is the exclusive influence in this area of law.

First, and consistently, the national courts have protected the confidentiality of commercially valuable information and business relationships for the sake of the market. The courts later went beyond this to protect certain private relationships of gradually expanding scope. They finally protected information that was confidential itself,[34] without a relationship of confidence and against any person. In this, the courts shifted towards an individual approach. In the 1980s and 1990s, the courts developed a set of state-facilitative doctrines: a ready acceptance of the public interest in the disclosure of confidential information to or by public authorities, distinctive duties of confidence owed to the Crown and a liberal approach to disclosure pursuant to statutory authority. There was no acknowledgment of discontinuity in approach or incoherence. Such developments run counter to narratives of the inexorable rise of the individual approach. State-restrictive elements coexisted within these developments, such as in the imposition of *Marcel* confidentiality on information gathered by

[34] *Attorney General v Guardian Newspapers (No 2)* [1990] 1 AC 109.

public authorities pursuant to their functions and the subjection of duties of confidence to the Crown to public interest tests for enforcement. This mixture of state-restrictive and state-facilitative approaches abruptly and surprisingly shifted towards a more state-restrictive approach in the Supreme Court in *Ingenious Media*. *Marcel* confidentiality was treated as a common law fundamental right and therefore the statutory power to disclose was interpreted narrowly: a State-restrictive approach.

The law of confidence reflects the influence of all four approaches to the public-private divide: the market approach underlies and endures, the individual approach has risen (ultimately to be overtaken by the development of the tort of misuse of public information), and the state-facilitative approach to information has been significantly reduced by a resurgent state-restrictive reading of the law in the Supreme Court. There is no evidence of outside pressures at work in these developments, such as Europe influence. Instead, they reflect choices of judicial architects of the public-private divide; choices which reflect a diversity of approach across its history.

EUROPEAN HUMAN RIGHTS

The history of Article 8 ECHR demonstrates a parallel development of state-restrictive and individual approaches to the public-private divide within the right to private life. It provides evidence of compromises struck between rival schools of thought and a mixture of approach within the public-private divide.

Even at the earliest stages in the development of Article 8 ECHR, both state-restrictive and individual approaches influenced legal developments. This was more so than traditional accounts of the development of human rights allow. The drafting history of Article 8 ECHR suggests that an individual approach to thinking about the public-private divide was already sufficiently influential to merit discussion and to provoke attempts to clarify the scope of Article 8(1) at the very beginning. The fact that an amendment to so clarify the effect of Article 8 ECHR, in favour of a state-restrictive approach, was rejected indicates the presence of disagreement among the drafters of Article 8 ECHR on this point. However, the compromise struck left the door open to a more expansive interpretation of Article 8(1). This possibility was indeed subsequently taken up by the ECtHR after 1998.

It is important not to exaggerate the willingness of the ECtHR to impose an individual approach to the public-private divide on the text of Article 8 ECHR. The development took a significant amount of time. Early jurisprudence adopted a state-restrictive approach. Positive obligations relating to information under Article 8 ECHR are only developments of the last 20 years. Understandings of the development of positive obligations as part of a fundamental shift away from the state-restrictive approach and towards an individual approach are

unsatisfactory. Neither was the development limited to a response to the privatisation of traditional state functions. It extended beyond the reformulation of a state-restrictive ambition to adapt to new relationships between public and private actors. The jurisprudence instead reveals the endurance of parallel state-restrictive and individual approaches within the ECtHR. Views that see the shift to an individual approach as always inherent in the nature of the human rights project neglect this mixture of approach within the jurisprudence. It is also important not to overstate the dominance of the individual approach in modern Article 8 ECHR jurisprudence. The ECtHR's role in this legal development was key.

The early development of positive obligations in Article 8 ECHR did little to alter the public-private divide. In 1986, the European Commission of Human Rights accepted a partially successful defamation action as adequate to show respect from private life.[35] It was not until the late 1990s that an individual approach started to exert any significant influence over information law in relation to Article 8 ECHR. Even then, dissenting opinions which objected to the existence of a negative/positive distinction and would have introduced a strong individual approach to Article 8 ECHR were not adopted by the ECtHR.[36] Instead, a more modest, though rising, individual approach to the public-private developed. First, this occurred in the European Commission of Human Rights in dicta comments in *Earl Spencer v United Kingdom*[37] and then more clearly in *Von Hannover v Germany* in 2005 by the ECtHR.[38] The positive obligations jurisprudence has remained relatively flexible and has accorded a margin of appreciation to the state.[39] It has not displaced the state-restrictive approach also present within the jurisprudence. Positive obligations continue to impose only a relatively low intensity review of the application of a civil action on states, to be resolved in conformity with the criteria laid down by the ECtHR, including a balancing exercise.[40] The flexibility of the ECtHR approach to private actors extends beyond media interference, where freedom of expression must be balanced with privacy, to the use of information by private employers in internal disciplinary investigations.[41] The rejection of dissenting voices in the ECtHR that would have removed the public-private divide in favour of "an obligation of

[35] *Winer v United Kingdom* App. No. 10871/84.
[36] See Dissenting Opinion of Judge Wilberhaber in *Stjerna v Finland* (1997) 24 EHRR 195.
[37] (1998) 24 EHRR CD105.
[38] (2005) 40 EHRR 1.
[39] See *Armoniene v Lithuania* (2009) 48 EHRR 53; *Mosley v United Kingdom* (2011) 53 EHRR 30.
[40] See *Von Hannover v Germany (No 2)* (2012) 55 EHRR 15.
[41] *Barbulescu v Romania* App. No. 61496/08; *Barbulescu v Romania* (Grand Chamber) App. No. 61496/08.

results" across the public-private divide shows that the ECtHR has not adopted a full individual approach to Article 8 ECHR.[42]

A state-restrictive public-private divide has endured, and indeed strengthened, despite the rise of the individual approach in ECHR jurisprudence. These developments reflect a vein of state-restrictive thinking within the ECtHR and a more limited adoption of the individual approach than might be expected were a more fundamental shift occurring. That the state-restrictive approach remains influential in the ECHR jurisprudence can be seen in a number of ways. There are good reasons to believe that several members of the ECtHR continue to favour a state-restrictive approach, even if a more limited set of compromises have been reached with the individual approach. The continuing judicial rhetoric of the court, its attitude to state surveillance, and the development of the doctrine of imputation in the context of Article 8 ECHR all indicate that a state-restrictive understandings endure. The mere mirroring of general international law on attribution and imputation is unlikely to explain the ECtHR's development of the doctrine of imputation: no reference is made to it, as one would expect if the ECtHR felt compelled to diverge from a unanimous preference for an individual approach. Further, the strange approach taken to imputation in *Masden v Denmark* is further evidence of the ECtHR negotiating a greater degree of internal disagreement and struggle.[43] Had there been a greater degree of consensus around an individual approach to imputation, the opportunity to develop the jurisprudence was a surprising one to miss. The ECtHR has also elaborated the negative obligation of the state to require standards of clarity, precise, detail and safeguards unseen in relation to the positive obligation on the state. The state-restrictive approach has therefore not only endured but has resurged in some respects in the ECHR jurisprudence.

Although there has been a significant erosion of the public-private divide in Article 8 ECHR jurisprudence, revealing the influence of an individual approach, the state-restrictive approach has remained vibrant alongside the individual approach. Rather than reflecting a gradual paradigm shift, the history of the public-private divide in Article 8 ECHR reveals the coexistence of different approaches within the jurisprudence.

NATIONAL HUMAN RIGHTS

State-restrictive, individual and state-facilitative approaches have all played an important role in the development of the public-private divide in national human rights law. While New Labour's Human Rights Act 1998 was drafted with a distinctive state-restrictive public-private

[42] See Dissenting Opinion of Judge Pinto De Albuquerque in *Barbulescu v Romania* App. No. 61496/08.
[43] (2003) 36 EHRR CD 61.

divide, albeit somewhat different from the public-private divide in ECHR jurisprudence, the divide was significantly eroded by the development of the tort of misuse of private information by national courts. Although this development was inspired and catalysed by the Human Rights Act 1998 and ECHR jurisprudence, its roots lie in an individual approach adopted by the national courts in the 1990s to confidentiality. There is evidence to suggest that the national courts were already developing the law in this direction and took advantage of human rights to accelerate that process in cooperation with the individual approach inherent in the European jurisprudence.

However, alongside this the national courts have introduced some divergent state-facilitative elements to national human rights law. They have also been willing to diverge from ECHR jurisprudence when developing the tort of misuse of private information. The ECHR jurisprudence and its criticism of the national jurisprudence was more influential, however, in requiring a resurgence of the state-restrictive approach in the national courts, where a more robust doctrine of "in accordance with the law" and necessity has developed in relation to state databases and processing. The state-restrictive approach has therefore resurged alongside the rise of an individual approach. This highlights the different effects of European influences on the development of the law: much stronger in relation to the national implementation of the state-restrictive negative obligations of States than the positive obligations jurisprudence. The implementation of Article 8 ECHR at the national level did not simply replicate ECHR jurisprudence. National courts resisted and diverged from ECHR jurisprudence in some places as well as implementing it in others.

EUROPEAN DATA PROTECTION

The history of European data protection reveals a much more complex interaction between different approaches to the public-private divide than a simple shift towards an individual approach. All four rival approaches to the public-private divide have been influential in the development of European data protection. The General Data Protection Regulation reflects the concerns of the market, individual, state-facilitative and state-restrictive approaches. The history of European data protection does not reflect struggle alone.

Early European data protection should be understood as the result of a rejection of the state-restrictive approach of early ECHR jurisprudence in favour of a more individual approach. This produced a range of national legislative responses with diverse approaches to data protection and the public divide. It was this rejection of the state-restrictive approach that produced the conditions in Europe that gave rise to support for the market approach from national Governments, tempered by state-facilitative exemptions. Rejection of the state-restrictive approach in favour of an individual approach catalysed market concerns which

were in turn tempered by state-facilitative exemptions. The Data Protection Directive was catalysed by the individual approach favoured by a network of data protection authorities in the late 1980s and early 1990s. This network instrumentalised market concerns, and the new powers available to the EC, to persuade the European Commission to act. Member State Governments once again acted to secure their interests through state-facilitative exemptions.

Later the ECJ and CJEU first reflected the market approach of the Directive before developing a more state-restrictive jurisprudence for the Data Protection Directive. This was in turn followed by the extension of protections against private data controllers, although to a lesser extent, reflecting an emergent individual approach under the influence of the ECHR and CFR. The jurisprudence shows shifts in approach over time.

Changes in European data protection post-Lisbon saw the market approach that dominated the Directive transcended by the recognition of data protection as a fundamental right. The drafting of the General Data Protection Regulation reflects individual and state-restrictive approaches to this fundamental right as well as state-facilitative exemptions successfully fought for by Member State Governments. Although market concerns form a baseline, several other approaches have transcended it. Although the individual approach has risen, the state-restrictive has resurged and state-facilitative approaches endured in particular fields alongside a baseline of market concerns.

National Data Protection

Although national data protection owes its broad shape and content to European data protection, national level divergence has occurred in several respects. Attempts to increase transparency and accuracy in the public sector and restore trust following the 2008 HMRC data breach scandal both contributed to a distinctive state-restrictive undercurrent in some parts of UK data protection.

National Governments before and during the 1970s were resistant to increases in data protection in the public sector and apathetic about its need in the private sector. National Governments reflected state-facilitative and market approaches to the public-private divide. The Conservative Government's embrace of data protection in the Data Protection Act 1984 owed much more to the 1981 Convention and its market approach, tempered by state-facilitative exemptions, than the individual approach that drove some national calls for data protection in the 1970s. The Data Protection Act 1998 was an implementation of the Data Protection Directive 46/95 EC but reflected a more market approach in several respects, diverging from the approaches in European law.

Important national divergence followed in response to demands for greater transparency in the early 2000s and control over the public sector following a series of data breaches in the late 2000s. National courts and tribunals developed the public-private divide in their jurisprudence on fair processing in the context of section 40(2) Freedom of Information Act 2000, making it easier to process personal data about officials in response to legitimate interests in transparency and accountability. The enforcement powers of the ICO also became more state-restrictive through reforms in the Coroners and Justice Act 2009, although it would be remiss to fail to observe the bundle of state-facilitative reforms in the Coroners and Justice Bill that failed to gain Parliamentary support. The Government's attempt to expand the power of public authorities to share data and reinforce a state-facilitative approach was defeated in a rare display of Parliamentary assertiveness, leaving only the state-restrictive safeguards from that package of reforms. The ICO's preference for an individual approach to these powers, extending to both the public and private sector, was not acted upon. Instead, business interests managed to persuade the Government that going beyond state-restrictive enforcement to include the private sector would impose an undesirable regulatory burden. The market approach's accepted compromise was in fact a state-restrictive conclusion in this instance and a state-facilitative ambition failed, leaving a state-restrictive remnant of the legislative package. National data protection law therefore illustrates well the complex interplay of differing approaches to the public-private divide in shaping the development of individual information law.

UNAUTHORISED DISCLOSURE OFFENCES

The complex and inconsistent framework for the criminalisation of unauthorised disclosures of official and other public authority information reflect struggles between the state-facilitative and state-restrictive approaches. These struggles have largely occurred between national Governments and Parliament, with a limited role for the courts. European institutions have done little to influence information law in this area, in contrast to human rights and data protection law, demonstrating the irregular and uneven impact of Europe over different fields of individual information law.

By the 1940s, a distinctively state-facilitative regime for the regulation of a wide range of official information had been created by Governments with little Parliamentary scrutiny. Its design centralised control over the disclosure of information by officials. The rise of a state-restrictive critique of official secrecy in the 1970s and 1980s resulted in the narrowing of official secrecy in Official Secrets Act 1989: a retreat of the state-facilitative approach. However, the core preserved by the Act reflected the survival of the state-facilitative approach. The national courts interpreted official secrecy legislation to resist more state-

restrictive approaches and the most recent Law Commission consultation on the Protection of Official Data has reflected a continuation of state-facilitative approaches to official secrecy. Media and civil society responses indicate that a fierce state-restrictive opposition exists and is willing to struggle against it.

An exclusive focus on official secrecy would result in neglecting the development of wider unauthorised disclosure offences. While a small number of such ad hoc statutory offences have been driven by market or individual concerns, and some by a genuine state-restrictive objective, the majority of offence demonstrate the endurance of a state-facilitative approach. Many of these offences were passed after 1989, as Governments slowly pushed to re-extend criminalisation to support public authority control of disclosure and to engender the trust necessary for public authorities to carry out their functions, without creating private sector equivalents.

A Historically-Grounded Theoretical Framework for understanding the Public-Private Divide

Complex interactions between the four approaches have shaped the public-private divide in individual information law. Various architects the public-private divide have shifted in their advocacy or support for different approaches. Different actors have played greater or lesser roles at different points in the history of individual information law. Developments have not been linear, or uniform, or consistent. The relationship between Europe and the UK, and the agency of the various architects of the public-private divide in individual information law, have been complex and nuanced. The history of UK individual information law, its Europeanisation, and national divergence and idiosyncrasy, reflect the interaction of approaches to the public-private divide that are identified and traced in this thesis.

Trends, however, can be discerned and commented upon within this. There has been a broad acceptance of the market approach to the regulation of information. It is difficult to see the future of information law ignoring the need to have a baseline of regulation to ensure the free flow of information across borders and to engender the trust of participants in the market. However, in many ways it has been transcended by the other approaches, remaining an interest of reactive and conservative voices that fear overregulation and excessive burdens on commerce. It finds some common ground with the individual approach, whose fortunes have risen and continue to rise. In more recent debates, one detects a readier conflation of the two. The argument that market confidence and the flow of information require strong protections for individual rights across the public-private divide has become more common. This was not always the case: the market approach has historically been concerned about the high standards of the individual approach. While state-

facilitative approaches have lost favour before courts, they endure and find favour with Governments, perhaps the institution most likely to see the benefit of a more lenient regime or special treatment for public authorities. As long as Governments dominate Parliament, we should expect to see a continuing push for state-facilitative exemptions in privacy and data protection and regimes for the regulation of official data. Finally, the history of the public-private divide has shown a surprising resurgence of the state-restrictive approach that had appeared to fall away between the 1970s and 1990s. That resurgence has, at different times and in relation to different parts of individual information law, been driven by judicial, legislative and executive actors.

THE ACCEPTANCE OF THE MARKET APPROACH

There is now broad acceptance of the market approach in data protection and confidentiality as a baseline, although it has only had limited influence on human rights and official secrecy. The market approach became highly influential in European data protection following the multiplication of piecemeal national legislative responses in the 1970s. Resolutions (73) 22 and Resolution (74) 29 of the Council of Europe, the 1981 Council of Europe Convention and the OECD Guidelines were motivated by concern for the free flow of information. Those concerns formed a major, if not exclusive, motivation behind the Data Protection Directive 46/95 EC and a substantial justification underpinning the EU General Data Protection Regulation. The resistance of the European Parliament to a public-private divide in 1992 was substantially driven by market concerns for the Data Protection Directive. Early ECJ jurisprudence reflected clear concerns of the market approach for the workability of the Directive. Nationally, both the Data Protection Act 1984 and Data Protection Act 1998 were primarily driven by this market imperative from Europe and in some respects for more market-orientated than European law. The doctrine of breach of confidence was built on jurisprudence with a core concern for commercial confidence and the protection of information to protect economic activity.

Although the market approach has widespread acceptance it has often been superseded by concerns of the individual or state-restrictive approaches. While a basic level of uniform protection is often granted for the sake of the market, concern for heighted protections for the individual, even where the market bears a greater regulatory burden, or state-restrictive and state-facilitative approaches, which emphasise non-market concerns have each proven more influential at different times.

Market approaches continue to appear in more recent developments but often as conservative reactions to changes proposed on the basis of other approaches. These often argue that a more restrictive approach will impose a disproportionate burden on business. It

is difficult to see this baseline concern for the free flow of information losing its importance in future debates over the regulation of individual information. Indeed, possibly the opposite will occur. It is a core feature accepted at the heart of the public-private divide in UK individual information law.

THE ENDURANCE OF THE STATE-FACILITATIVE APPROACH

The state-facilitative approach has endured throughout the history of the public-private divide. In the "absence of multiple veto points and the presence of supportive institutions", such as nationally with a dominant executive and supportive Parliament, Governments have been free to introduce state-facilitative exemptions or regimes.[44] Where Governments have benefited from vetoes at the European level, they have successfully extracted state-facilitative exemptions, which helps to explain why Governments have successfully pursued this approach at both the European and national level.

Isolated examples of the state-facilitative approach can be found in the jurisprudence of the ECHR but there is no general pattern.[45] The law of confidence in the national courts was broadly state-facilitative in the 1970s and 1990s, with disclosure in the public interest where it was reasonably connected to public functions and state-facilitative duties of confidence to the Crown. However, with the development of the tort of misuse of private information and recognition of *Marcel* confidentiality as a fundamental common law right, the national courts have moved away from the state-facilitative approach to a mixture of individual and state-restrictive approaches.

National Governments, on the other hand, have frequently sought to introduce state-facilitative exemptions to mitigate the full rigours of information law. This can be seen across the history of data protection in Resolutions (73) 22 and Resolution (74) 29 of the Council of Europe, the 1981 Council of Europe Convention, the 1981 OECD Guidelines, Data Protection Act 1984, Data Protection Directive 46/95 EC, and the Data Protection Act 1998. Later reforms of the Data Protection Act 1998, in response to major public-sector data breaches, though state-restrictive in effect, were in fact intended to restore trust in public authorities. Those reforms themselves were part of a broader, ultimately failed, attempt to introduce a comprehensive and wide power to enable public authorities to share information: a state-facilitative project. The history of official secrecy and other legislative secrecy regimes and wrongful disclosure offences is replete with examples of state-facilitative approaches being championed by Governments.

---

[44] Borzel, "Conceptualising the Domestic Impact of Europe", in Featherstone and Radaelli (eds.) (2003), p. 74.
[45] See chapter 3, pp. 76.

So long as national Governments can dominate Parliament and Governmental support is required for the success of European and international regimes, the state-facilitative approach is likely to endure. It is a core feature enduring at the heart of the public-private divide in information law, supported by executive and legislative actors.

THE RISE OF THE INDIVIDUAL APPROACH

Individual approaches to the public-private divide have been present from the beginning. They were present in the drafting debates surrounding the ECHR and in national responses to the perceived inadequacy of the ECHR in the 1970s. From humble beginnings, it has enjoyed an impressive rise to prominence, but not dominance. Undoubtedly, this improvement in the fortunes of an individual approach to the public-private divide in individual information law represents the fruits of reflection on the implications of rapid technological change and the greater interconnection between public authorities and private actors that results from the greater flow of information and structural blurring of the public-private divide. My argument is not that these trends are not important, but that they do not vindicate deterministic claims about the trajectory of the public-private divide.

The rise of the individual approach in Article 8 ECHR is perhaps the clearest and most commented upon instance of this trend. The recognition by the ECtHR of positive obligations to regulate private actors across a variety of rights did a great deal to erode the public-private divide. In relation to information, its effect was only significant in human rights after 1998. Positive obligations on the state to secure respect for private life, even between private actors, were a major jurisprudential development and positive obligations are now widespread and varied in ECtHR jurisprudence. From the mere recognition that the absence of an actionable remedy to protect private life from interference by private actors could breach the positive obligation under Article 8 ECHR in *Earl Spencer v UK*, positive obligations have moved to clear recognition in *Von Hannover v Germany*.[46] In the latter case, the ECtHR emphasised that the applicable principles in relation to both negative and positive obligations were "similar".[47] In *Von Hannover v Germany (No 2)*, the ECtHR elaborated the requirements of a civil action to protect Article 8 ECHR rights from violations by private actors and the supervisory review the ECtHR would exert over such decisions.[48] The Grand Chamber in *Barbulescu v Romania* have continued this trend of applying the individual approach in relation to private actors.[49]

---

[46] (1997) 24 EHRR 195 and (2005) 40 EHRR 1.
[47] (2005) 40 EHRR 1, para. 58.
[48] (2012) 55 EHRR 15.
[49] App. No. 61496/08.

The rise of the individual approach is also crucial to understanding the development of European data protection. The proliferation of diverse national approaches in response to criticism of the state-restrictive approach to Article 8 ECHR jurisprudence in the 1960s catalysed the development of early European data protection. Although the market approach was responsible for early European data protection and persisted in later European data protection, this process was initiated by the rise of the individual approach. Transnational data protection authority networks, motivated by an individual approach, instrumentalised market concerns to encourage the European Communities to legislate in the 1990s. The rise of data protection in the Charter of Fundamental Rights and the Lisbon Treaty reflect the work of fundamental rights advocates and produced the much stronger protections of the General Data Protection Regulation. In the national courts, the individual approach has become increasingly important to the law of breach of confidence from the early recognition of personal relationships as capable of protection from private actors to the development of the tort of misuse of private information, supported by the Human Rights Act 1998 and developing ECHR jurisprudence.

Though present from the beginning, the individual approach is a core and rising feature of the public-private divide in the UK individual information law. It is increasingly influential across legislative, judicial and regulatory actors.

The Resurgence of the State-Restrictive Approach

Finally, the state-restrictive approach has not only endured but resurged in the recent history of the public-private divide in information law. The surprising result runs contrary to narratives that consider it to be a historical anachronism and its presence in the law a historical remnant to be gradually overcome. It has resurged as a core feature of the public-private divide in individual information law.

The state-restrictive approach, dominant in the drafting of and the early jurisprudence of the ECHR, was not abandoned. This was so even during a period of significant jurisprudential development in response to an individual approach. In more recent jurisprudence it has in fact strengthened. This is especially apparent in relation to the development of jurisprudence on the requirement that public authority interferences with the right to private life are “in accordance with the law” and “necessary in a democratic society”. It persists in the rhetoric of the ECtHR, the treatment of state surveillance, and the approach of the ECtHR to the doctrine of imputation. Article 8 ECHR requires standards of precision, detail, foreseeability and accessibility, with substantive safeguards and effective controls, quite beyond those required by the national law regulating private actors. The ECtHR has strengthened this requirement at the same time as developing positive obligations.

After an initially market approach to interpretation, the ECJ and CJEU developed a more state-restrictive approach in their jurisprudence on the 1995 Directive. They did this first by subjecting processing under Article 7(c) and (e) to Article 8 ECHR jurisprudence as a "general principle of law". Later they subjected such processing to Articles 7 and 8 CFR. Although the CJEU has more recently extended fundamental rights review to private entities processing, it has not matched the intensity and structure of review for public authorities. It remains predominantly a state-restrictive jurisprudence, although showing the influence of an individual approach as well. The state-restrictive approach has resurged in the General Data Protection Regulation, especially in relation to the clear restriction of processing necessary for the legitimate interests to bodies which are not public authorities in the performance of their tasks.

In relation to the protection of confidential information, the national courts have most recently taken a distinctive turn in favour of a state-restrictive approach, recognising *Marcel* confidentiality as a common law fundamental right. They therefore insist on the narrow interpretation of statutory powers that restrict that right. This is in contrast to the more state-facilitative approach of the national courts in the 1990s.

In national data protection, Government, Parliament and national courts and tribunals have all contributed to divergence from European data protection by adopting more state-restrictive approaches to ICO enforcement powers and transparency. In national human rights, pushed and prompted by the ECHR, national courts have become more state-restrictive in relation to public authority databases, search powers and disclosures.

The resurgence of the state-restrictive approach is clear and important evidence that the public-private divide is not simply being eroded by concerns and developments motivated by an individual approach. The state-restrictive approach is a core feature at the heart of the public-private divide in UK information law which has resurged in multiple parts of the law.

UNDERSTANDING THE PAST AND LOOKING TO THE FUTURE

This thesis has provided a historically-grounded theoretical framework for understanding and reflecting upon the public-private divide in UK information law during a period of significant technological, social and political change. The market, individual, state-restrictive and state-facilitative approaches help to explain complex interactions that have shaped the history of the public-private divide. Its history is more complex and nuanced than a shift towards to individual approach or struggle alone. The different approaches identified in this thesis have profoundly shaped the public-private divide in individual information law across its history and are woven throughout the current law. Understanding individual information law and the

public-private divide first requires an understanding of this complex interaction and history. It is necessary if we are to engage effectively in debates about its future.

BIBLIOGRAPHY

BOOKS

Lee Bygrave, Data Privacy Law: An International Perspective (2014)

Lee Bygrave, Legal Scholarship on Data Protection: Future Challenges and Directions, in Terwangne, Degrave, Dusollier and Quick (eds.), Liber Amicorum Yves Pollet: Essays in Honour of Yves Pollet (2018)

Manuel Castells, The Rise of the Network Society (1996)

Francis G Castles, The Future of the Welfare State: Crisis Myths and Crisis Realities (2004)

Francis G Castles, Stephen Leibfried, Jane Lewis, Herbert Obinger and Christopher Pierson (eds.), The Oxford Handbook of the Welfare State (2010)

Diane Coyle, Economics: The Weightless Economy (1997)

Marco Duranti, The Conservative Human Rights Revolution (2017)

Kevin Featherstone and Claudio Radaelli (eds.), The Politics of Europeanization (2003)

David Feldman, Civil Liberties and Human Rights in England and Wales (2005)

Anthony Giddens, The Third Way: The Renewal of Social Democracy (1998)

Gloria Gonzalez Fuster, The Emergence of Personal Data Protection as a Fundamental Right of the EU (2011)

Simon Garfinkel, Database Nation: The Death of Privacy in the 21st Century (2000)

Neil Gilbert, Transformation and the Welfare State: The Silent Surrender of Public Responsibility (2002)

Bill Gates, The Road Ahead (1996)

Friedrich Hayek, The Road to Serfdom (1944)

Edward Higgs, The Information State in England: The Central Collection of Information on Citizens Since 1500 (2003)

Frits W Hondius, Emerging Data Protection in Europe (1975)

Frits W Hondius, The Human Rights Aspect of Data Protection (1985)

Rosemary Jay, Data Protection Law and Practice (2012)

David Kennedy, A World of Struggle: How Power, Law, and Expertise Shape Global Political Economy (2016)

Julian Le Grand, Motivation, Agency and Public Policy: Of Knights and Knaves, Pawns and Queens (2003)

Orla Lynskey, The Foundations of EU Data Protection Law (2015)

Milton Friedman, Capitalism and Freedom (1962)

Christopher May, The Information Society: A Sceptical View (2002)

Michael Moran, The British Regulatory State: High Modernism and Hyper-Innovation (2003)

Alastair Mowbray, The Development of Positive Obligations under the European Convention on Human Rights by the European Court of Human Rights (2004)

Abraham Newman, Privacy and Regulation in a Digital Age, in Bouwman, Preissl and Steinfield (eds.), E-Life After the Dot.Com Bust (2004)

Nicholas Negroponte, Being Digital (1995)

Andrew Newman, Privacy Protection in Europe: Administrative Feedbacks and Regional Politics, in Meunier and McNamara (eds.), The State of the European Union (2007)

Danny Nicol, The Constitutional Protection of Capitalism (2010)

Helen Nissenbaum, Privacy in Context: Technology, Policy and the Integrity of Social Life (2010)

David Osbourne and Ted Gaebler, Reinventing Government: How the Entrepreneurial Spirit is Transforming the Public Sector (1992)

Paul Pierson, Dismantling the Welfare State? Regan, Thatcher and the Politics of Retrenchment (1994)

Paul Pierson, The New Politics of the Welfare State (2001)

Daniel Solove, The Digital Person: Technology and Privacy in the Information Age (2004)

Daniel Solove, Understanding Privacy (2008)

Evan Stubbs, Big Data, Big Innovation: Enabling Competitive Differentiation Through Business Analytics (2014)

Alvin Toffler, The Third Wave (1980)

Raymond Wacks, The Protection of Privacy (1980)

Dimitris Xenos, The Positive Obligations of the State Under the European Convention of Human Rights (2012)

ARTICLES

John Allison, History in the Law of the Constitution (2007) 28 Journal of Legal History 263

John Allison, History to Understand, and History to Reform, English Public Law (2013) CLJ 526

Tanya Aplin, The Development of the Action for Breach of Confidence in a Post-HRA Era (2007) Intellectual Property Quarterly 19

Jack M Balkin, The Constitution in the National Surveillance State (2008) 93 Minn. L. Rev. 1

Nicholas Bamforth, The Application of the Human Rights Act 1998 to Public Authorities and Private Bodies (1999) CLJ 159

Nicholas Bamfoth, The True Horizontal Effect of the HRA 1998 (2001) LQR 34

Nicholas Barber, Privacy and the Police: Private Right, Public Right or Human Right? [1998] Public Law 19

Julia Black, The Emergence of Risk-Based Regulation and the New Public Risk Management in the United Kingdom [2005] Public Law 512

Peter Blume, Privacy as a Theoretical and Practical Concept (1997) 11(2) International Review of Law, Computers and Technologies 193

Peter Blume, Data Protection in the Private Sector (2004) 47 Scandinavian Stud. L. 297

Peter Blume, The Public Sector and the Forthcoming EU Data Protection Regulation (2015) EDPL 32

Oliver Butler, Confidentiality and Public Authorities: Fundamental Rights, Legality and Disclosure for Statutory Functions (2017) 76(2) CLJ 253

Oliver Butler, Obligations Imposed on Private Parties by the GDPR and UK Data Protection Law: Blurring the Public-Private Divide (2018) 24(3) European Public Law 555

Richard Buxton, The Human Rights Act and Private Law (2000) 116 LQR 48

AIL Campbell, Positive Obligations under the ECHR: Deprivation of Liberty by Private Actors (2006) (10) Edinburgh Law Review 399

Jean-Paul Costa, The European Court of Human Rights: Consistency of its Case Law and Positive Obligations (2008) 26 Netherlands Quarterly Human Rights 449

Stephen Daly, R (Ingenious Media) v HMRC: Public Disclosures and HMRC's Duty of Confidentiality (2017) British Tax Review 10

Elizabeth Denham, Transparency, Trust and Progressive Data Protection (29 September 2016) at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/09/transprency-trust-and-progressive-data-protection/

Brice Dickson, Positive Obligations and the European Court of Human Rights (2010) 61(3) NILQ 203

Oliver Digglemann and Maria Nicole Cleis, How the Right to Privacy Became a Human Right (2014) (14) Human Rights Law Review 441

Catherine Donnelly, Positive Obligations and Privatisation (2010) 61 Northern Ireland Legal Quarterly 209

David Feldman, The Developing Scope of Article 8 of the European Convention on Human Rights (1997) EHRLR 265

John Glover, Is Breach of Confidence a Fiduciary Wrong? Preserving the Reach of Judge-Made Law" (2001) Legal Studies 594

Klaus Goetz, Four Words of Europeanisation, paper prepared for the ECPR Joint Sessions of Workshops, Turin, Italy (7th March 2002)

Andrew Goodall, Taxpayer Confidentiality: Harnett sets out HMRC View for MPs, Tax Journal (21 October 2011)

John Griffith, The Political Constitution (1979) 42 MLR 1

Cees Hamelink, "Is there Life after the Information Revolution?", in Michael Trabner (ed.), The Myth of the Information Revolution: Social and Ethical Implications of Communication Technology (1986)

Joe Handler and Margaret Rosenheim, Privacy in Welfare: Public Assistance and Juvenile Justice (1966) 31 Law and Contemporary Problems 377

Kirsty Hughes, Horizontal Privacy (2009) LQR 244

Murray Hunt, The Horizontal Effect of the HRA [1998] Public Law 423

Niilo Jaaskinen, Europeanisation of National Law: A Legal-Theoretical Analysis (2015) European Law Review 667

Richard Kay, The European Convention on Human Rights and the Control of Private Law (2005) EHRLR 466

Ursula Kilkelly, Protecting Children's Rights under the ECHR: the Role of Positive Obligations (2010) 61 Northern Ireland Legal Quarterly 245

Anthony Lester and David Pannick, The Impact of the Human Rights Act on Private Act: The Knight's Move (2000) 116 LQR 380

Andrew Mackenzie, Privacy – a New Right in UK Law? (2002) Scots Law Times 98

Giandomenico Malone, The Rise of the Regulatory State in Europe (1994) 17(3) West European Politics 77

Giandomenico Malone, From the Positive to the Regulatory State: Causes and Consequences of Change in the Mode of Governance (1997) 17(2) Journal of Public Policy 139

Basil Markesinis, Privacy, Freedom of Expression, and the Horizontal Effect of the Human Rights Bill: Lessons from Germany (1999) LQR 47

Osita Mba, Transparency and Accountability of Tax Administration in the UK: the Nature and Scope of Taxpayer Confidentiality (2012) British Tax Review 187

Andrew Newman, Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive (2008) 62(1) International Organization 103

Rory O'Connell, Realising Political Equality: the European Court of Human Rights and Positive Obligations in a Democracy (2010) 61 NILQ 263

Dawn Oliver, The Frontiers of the State: Public Authorities and Public Function under the Human Rights Act 1998 [2000] Public Law 476

Stephanie Palmer, In the Interests of the State: the Government's Proposals for Reforming Section 2 of the Official Secrets Act 1911 [1988] Public Law 523

Stephanie Palmer, Public, Private and the Human Rights Act 1998: An Ideological Divide (2007) CLJ 559

Stephanie Palmer, Public Functions and Private Services: A Gap in Human Rights Protection (2008) 6 International Journal of Constitutional Law 585

Graham Pearce and Nicholas Plattern, Achieving Personal Data Protection in the European Union (1998) 36(4) Journal of Common Market Studies 529

Gavin Phillipson, The Human Rights Act, Horizontal Effect and the Common Law: A Bang or a Whimper (1999) 62 MLR 824

Gavin Phillipson and Helen Fenwick, Breach of Confidence as a Privacy Remedy in the Human Rights Era (2000) 63 MLR 600

Gavin Phillipson, Transforming Breach of Confidence – Towards a Common Law Right of Privacy under the Human Rights Act (2003) 66 MLR 726

Gavin Phillipson, Judicial Reasoning in breach of Confidence Cases under the Human Rights Act: Not Taking Privacy Seriously? (2003) EHRLR 54

Gavin Phillipson and Alexander Williams, Horizontal Effect and the Constitutional Constraint (2011) 74 MLR 878

Gavin Phillipson, "Privacy and Breach of Confidence: The Clearest Case of Horizontal Effect?" in D. Hoffmann (ed.) The Impact of the UK Human Rights Act on Private Law (2011)

Maija Pitkänen, Fair and Balanced Positive Obligations – Do They Exist? (2012) EHRLR 538

Helen Quane, The Strasburg Jurisprudence and the Meaning of a 'Public Authority' under the Human Rights Act [2006] Public Law 106

Neil Richards, The Dangers of Surveillance (2012-2013) 126 Harvard Law Review 1934

David Russell, Supplementing the European Convention on Human Rights: Legislating for Positive Obligations (2010) 61 NILQ 281

Colin Scott, Analysing Regulatory Space: Fragmented Resources and Institutional Design (2001) Public Law 329

Victoria Schwartz, Overcoming the Public-Private Divide in Privacy Analogies (2015) Hastings Law Journal 143

Rabinder Singh, Using Positive Obligations in Enforcing Rights (2008) 13 Judicial Review 94

Spiros Simitis, From the Market to the Polis: The EU Directive on the Protection of Personal Data (1994-1995) 80 Iowa L Rev 445

ATH Smith, Security Services, Leaks and the Public Interest [2002] CLJ 514

Iain Steele, Public Law Liability – the Human Rights Act and Beyond (2005) CLJ 8

Nick Taylor, Policing, Privacy and Proportionality (2003) European Human Rights Review 86

Rosamund M Thomas, The British Official Secrets Acts 1911-1939 and the Ponting Case [1986] Criminal Law Review 491

Paul Vincent-Jones, The Regulation of Contractualisation in Quasi-Markets for Public Services (1999) Public Law 304

William Wade, Horizons of Horizontality (2000) 116 LQR 217

Alexander Williams, A Fresh Perspective on Hybrid Public Authorities under the Human Rights Act 1998: Private Contractors, Rights-Stripping and 'Chameleonic' Horizontal Effect (2011) Public Law 139

Alexander Williams, Strasbourg's Public-Private Divide and the British Bill of Rights [2015] EHRLR 617

Jane Wright, A Damp Squib? The Impact of Section 6 HRA on the Common Law: Horizontal Effect and Beyond [2014] Public Law 289

Shelly Wright, Confidentiality and the Public/Private Dichotomy (1993) European Intellectual Property Review 237

CASES

Entick v Carrington 95 ER 807

Pollard v Photographic Co (1888) 40 Ch D 345

Weld-Blundell v Stephens [1919] 1 KB 520

Tournier v National Provincial and Union Bank of England [1924] 1 KB 461

Saltman Engineering Co v Campbell Engineering Co (1948) 65 RPC 203

Terrapin Ltd v Builders Supply Co (Hayes) Ltd [1960] RPC 128

Paul (Printing Machinery) Ltd v Southern Instruments (Communications) Ltd [1964] RPC 118

Bostitch Inc v McGarry and Cole Ltd [1964] RPC 173

Chandler v DPP [1964] AC 763

Seager v Copydex Ltd [1967] 1 WLR 923

Suhner and Co AG v Transradio Ltd [1967] RPC 329

Boardman v Phipps [1967] 2 AC 46

Argyll v Argyll [1967] Ch 302

Initial Services Ltd v Putterill [1968] 1 QB 396

Coco v AN Clark (Engineers) Ltd [1969] RPC 41

Fraser v Evans [1969] 1 QB 349

Butler v Board of Trade [1971] Ch 680

Hubbard v Vosper [1972] 2 QB 84

Church of Scientology v Kaufman [1973] RPC 627

Beloff v Pressdram [1973] FSR 33

Attorney General v Jonathan Cape [1976] QB 752

Woodward v Hutchins [1977] 1 WLR 760

Malone v Metropolitan Police Commissioner [1979] Ch 344

Tyrer v United Kingdom (1979-1980) 2 EHRR 1

Klass v Germany (1979-1980) 2 EHRR 214

Sunday Times v United Kingdom (1979-1980) 2 EHRR 245

Marckx v Belgium (1979) 2 EHRR 330

Airey v Ireland (1979-1980) 2 EHRR 305

Schering Chemicals Ltd v Falkman Ltd [1982] QB 1

Inland Revenue Commissioners v National Federation of Self-Employed and Small Businesses Ltd [1982] AC 617

A v Germany (1983) 5 EHRR CD292

Silver v United Kingdom (1983) 5 EHRR 347

Francome v Mirror Group Newspapers [1984] 1 WLR 892

A v United Kingdom (1984) 6 EHRR CD583

Malone v United Kingdom (1985) 7 EHRR 14

Lion Laboratories v Evans [1985] QB 526

X and Y v Netherlands (1985) 8 EHRR 235

Winer v United Kingdom App. No 10871/84 (10 July 1986)

Leander v Sweden (1987) 9 EHRR 433

Stephens v Avery (1988) 11 IP 439

Re A Company's Application [1989] Ch 477

Chappell v United Kingdom (1990) 12 EHRR 1

Huvig v France (1990) 12 EHRR 528

Kruslin v France (1990) 12 EHRR 547

W v Egdell [1990] Ch 359

Re Smith Kline and French Laboratories [1990] 1 AC 64

Attorney General v Guardian Newspapers (No 2) [1990] 1 AC 109

Lord Advocate v The Scotsman [1990] 1 AC 812

Kaye v Robertson [1991] FSR 62

Marcel v Metropolitan Police Commissioner [1992] Ch 225

Hoechst UK Ltd v Chemiculture Ltd [1993] FSR 270

Niemietz v Germany (1993) 16 EMRR 97

Funke v France (1993) 16 EHRR 297

Miailhe v France (1993) 16 EHRR 332

Ludi v Switzerland (1993) 15 EHRR 173

Herczegfalvy v Austria (1993) 15 EHRR 437

JS v United Kingdom App. No. 191173/91 (3 January 1993)

Shelly Films v Rex Features Ltd [1994] EMLR 134

Esbester v United Kingdom (1994) 18 EHRR CD72

Murray v United Kingdom (1995) 19 ECHR 193

Hellewell v Chief Constable of Derbyshire [1995] 1 WLR 804

Re Arrows (No 4) [1995] 2 AC 75

Vereniging Radio 100 v Netherlands (1996) 22 EHRR CD198

Creation Records Ltd v News Group Newspapers Ltd [1997] EMLR 444

Stjerna v Finland (1997) 24 EHRR 195

Barrymore v News Group Newspapers Ltd [1997] FSR 600

Earl Spencer v United Kingdom (1998) 25 EHRR CD105

Camenzind v Switzerland (1999) 28 EHRR 458

Lambert v France (2000) 30 EHRR 346

Amann v Switzerland (2000) 30 EHRR 843

Woolgar v Chief Constable of Sussex Police [2000] 1 WLR 25

R v Secretary of State for the Home Department, ex p Simms [2000] 2 AC 115

Rotaru v Romania [2000] ECHR 192

Attorney General v Blake [2001] 1 AC 268

R (Ford) v Press Complaints Commission [2001] EWHC Admin 683

London Regional Transport v Mayor of London [2001] EWCA Civ 1491

Khan v United Kingdom (2001) 31 EHRR 45

Petra v Romania (2001) 33 EHRR 5

Venables v New Group Newspapers (No 2) [2001] Fam 430

R v Shayler [2001] EWCA Crim 1977

Douglas v Hello! [2001] QB 967

Tamosius v United Kingdom (2002) 35 EHRR CD323

Theakston v MNG Ltd [2002] EWHC 137 QB

R v Shayler [2002] UKHL 11

Aston Cantlow and Wilcote with Billesley Parochial Church Council v Wallbank [2003] UKHL 37.

Anufrijeva v Southwark Borough Council [2003] EWCA Civ 1406; [2004] QB 1124

Chalkley v United Kingdom (2003) 31 EHRR 30

Giovine v Italy (2003) 36 EHRR 8

Peck v United Kingdom (2003) 36 EHRR 41

Masden v Denmark (Admissibility) (2003) 36 EHRR CD61

Martin v United Kingdom (Admissibility) (2003) 37 EHRR CD91

Hewitson v United Kingdom (2003) 37 EHRR 31

Natoli v Italy (2003) 37 EHRR 49

X v SO [2003] EWHC QB 1101

A v B Plc [2003] QB 195

C-465/00 *Rechnugshof v Osterreichischer Rundfunk* (2003) ECR I-04989

C-101/01 *Criminal Proceedings Against Bodil Lindqvist* (2003) ECR I-12971

Avocet Hardeware Plc v Morrison EAT/0417/02/DA (17 February 2003)

Campbell v MGN Ltd [2004] 2 AC 406

Campbell v MGN Ltd [2004] UKHL 22

Lewis v United Kingdom (2004) 39 EHRR 9

MM v Netherlands (2004) 39 EHRR 19

Ernst v Belgium (2004) 39 EHRR 35

Craxi v Italy (2004) 38 EHRR 19

Wainwright v Home Office [2004] 2 AC 406

(R) Marper v Chief Constable of South Yorkshire Police [2004] 1 WLR 2196

Von Hannover v Germany (2005) 40 EHRR 1

Doerga v Netherlands (2005) 41 EHRR 4

Storck v Germany (2006) 43 EHRR 6

McKennitt v Ash [2006] EWCA Civ 1714

Douglas v Hello! (No 6) [2006] QB 125

Ministry of Defence v Information Commissioner EA 2006 0027

A v Information Commissioner EA 2006 0022

London Borough of Bexley v Information Commissioner EA 2006 0060

Ministry of Defence v Information Commissioner EA 2006 0027

YL v Birmingham City Council [2007] UKHL 27

Elahi v United Kingdom (2007) 44 EHRR 30

Copland v United Kingdom (2007) 44 EHRR 37

Corporate Officer of the House of Commons v Information Commissioner 2007 WL 9362171

Department for Business, Enterprise and Regulatory Reform v Information Commissioner EA 2007 0072

London Borough of Camden v Information Commissioner EA 2007 0021

Weber and Saravia v Germany (2008) 46 EHRR SE5

Wieser v Austria (2008) 46 EHRR 54

S and Marper v United Kingdom (2008) 48 EHRR 1169

Douglas v Hello! (No 3) [2008] 1 AC 1

Mosley v Express Newspapers Plc [2008] EWHC 1777 QB

C-524/06 *Heinz Huber v* Bundesrepublik *Deutschland* (2008) ECR I-09705

Corporate Officer of the House of Commons v Information Commissioner [2008] EWHC 1084 (Admin)

Johnson v Medical Defence Union Ltd (No 2) [2008] Bus LR 503

Guardian News and Media Ltd v Information Commissioner EA 2008 0084

Liberty v United Kingdom (2009) 48 EHRR 1

Van Vondel v Netherlands (2009) 48 EHRR 12

Armoniene v Lithuania (2009) 48 EHRR 53

Murray v Express Newspapers Plc [2009] Ch 481

Clift v Slough Borough Council [2009] EWHC 1550 (QB)

Thackeray v Information Commissioner EA 2009 0063

Bousfield v Information Commissioner EA 2009 0113

Gillan and Quinton v United Kingdom (2010) 50 EHRR 45

C-92/09 *Volker and Markus Schecke GbR v Land Hessen* ECLI:EU:C:2010:353 (AG Opinion) (17 June 2010)

C-28/08 *European Commission v Bavarian Lager* EU:C:2010:378 (29 June 2010)

C-92/09 *Volker and Markus Schecke GbR v Land Hessen* ECLI:EU:C:2010:662 (9 November 2010)

Greenwood v Information Commissioner EA 2010 0007

Guardian Newspapers Ltd v Information Commissioner EA 2010 0070

Davis v Information Commissioner EA 2010 0024

Dun v Information Commissioner EA 2010 0060

Pycroft v Information Commissioner EA 2010 0165

T W Gibson v Information Commissioner EA 2010 0165

R (GC) v Commissioner of Police of the Metropolis [2011] UKSC 21

General Dental Council v Savery [2011] EWHC 3011 (Admin)

Kennedy v United Kingdom (2011) 52 EHRR 4

Aleksanyan v Russia (2011) 52 EHRR 18

Mosley v United Kingdom (2011) 53 EHRR 30

CTB v News Group Newspapers Ltd [2011] EWHC 1326 (QB) and 1334 (QB)

C-468/10 *ASNEF v Administracion de Estado* (2011) ECR I-12181

R (Ali) v Minister for the Cabinet Office [2012] EWHC 1943 (Admin)

Iordachi v Moldova (2012) 54 EHRR 5

Von Hannover v Germany (No 2) (2012) 55 EHRR 15

Trago Mills (South Devon) Ltd v Information Commissioner EA 2012 0028

R (Ingenious Media) v Commissioners for Revenue and Customs [2013] EWHC 3258 (Admin)

ZY v Higgins [2013] NIQB 8

Ageyevy v Russia App. No. 7075/10 (18 April 2013)

Callus v Information Commissioner EA 2013 0159

MM v United Kingdom The Times, 16 January 2013

R (T) v Chief Constable of Greater Manchester Police [2014] UKSC 35

Shimovolos v Russia (2014) 58 EHRR 26

C-131/12 *Google Spain SL v Agencia Espanola de Proteccion de Datos (AEPD)* ECLI:EU:C:2014:317 (13 May 2014)

Surrey Health Borough Council v Information Commissioner [2014] UKUT 0339 (AAC)

Edem v Information Commissioner [2014] EWCA Civ 92

In re Z (Children) (DNA Profiles: Disclosure) [2015] EWCA Civ 34

R (Catt) v Association of Chief Police Officers of England, Wales and Northern Ireland [2015] UKSC 9

Roberts v Commissioner of the Metropolis [2015] UKSC 79

Vidal-Hall v Google Inc [2015] 3 WLR 409

LH v Latvia (2015) EHRR 17

R (Ingenious Media) v Commissioners for Revenue and Customs [2015] EWCA Civ 173; [2015] 1 WLR 3183

Representative Claimants v MGN Ltd [2015] EWCA Civ 1291

R (JK) v The Registrar General for England and Wales [2015] EWHC 999 (Admin); [2016] 1 All ER 354

C-293/12 *Digital Rights Ireland* and C-203/15 *Tele2 Sverige AB* [2015] QB 127

C-698/15 *Secretary of State for the Home Department v Watson* ECLI:EU:C:2016:970 (21 December 2016)

Couderc v France [2016] EMLR 19

MN v San Marino (2016) 62 EHRR 19

Dragojevi v Croatia (2016) 62 EHRR 25

Zakharov v Russia (2016) 63 EHRR 17

RE v United Kingdom (2016) 63 EHRR 2

Szabo and Vissy v Hungary (2016) 63 EHRR 3

Barbulescu v Romania App. No. 61496/08

R (Ingenious Media) v Commissioners for Revenue and Customs [2016] UKSC 54; [2016] 1 WLR 164

PJS v News Group Newspaper [2016] UKSC 26

Axon v Ministry of Defence [2016] EWHC 787 (QB)

Burrell v Clifford [2016] EWHC 294 (QB)

J20 v Facebook [2016] NIQB 98

Mohamud v WM Morrison Supermarkets plc [2016] UKSC 11

Cox v Ministry of Justice [2016] UKSC 10

Big Brother Watch v United Kingdom App. No. 24960/15

LEGISLATION

Income Tax Act 1799

Official Secrets Act 1889

Official Secrets Act 1911

Official Secrets Act 1920

Official Secrets Act 1939

Atomic Energy Act 1946

Coal Industry Nationalisation Act 1946

Industrial Organisation and Development Act 1947

Statistics of Trade Act 1947

Prevention of Damage by Pests Act 1949

Agricultural Marketing Act 1958

Rivers (Prevention of Pollution) Act 1961

Harbours Act 1964

Gas Act 1965

Medicines Act 1968

Data Surveillance Bill 1969

Personal Records (Computers) Bill 1969

Sea Fish Industry Act 1970

Control of Personal Information Bill 1971

Counter-Inflation Act 1973

Employment Agencies Act 1973

Health and Safety at Work Act 1974

Rehabilitation of Offenders Act 1974

Carriage of Goods (Prohibition of Discrimination) Regulations 1977/276

Highways Act 1980

Fisheries Act 1981

Public Passenger Vehicles Act 1981

Civil Aviation Act 1982

Industrial Training Act 1982

Iron and Steel Act 1982

Merchant Shipping (Liner Conferences) Act 1982

Telecommunications Act 1984

Building Act 1984

Data Protection Act 1984

Police and Criminal Evidence Act 1984

Companies Act 1985

Airports Act 1986

Companies Act 1989

Electricity Act 1989

Water Act 1989

Official Secrets Act 1989

Finance Act 1989

Broadcasting Act 1990

Town and Country Planning Act 1990

Child Support Act 1991

Criminal Justice Act 1991

Water Industry Act 1991

Water Resources Act 1991

Social Security and Administration Act 1992

Cardiff Bay Barrage Act 1993

National Lottery Act 1993

Railways Act 1993

Criminal Justice and Public Order Act 1994

Goods Vehicles (Licensing of Operators) Act 1995

Shipping and Trading Interests (Protection) Act 1995

Criminal Appeal Act 1995

Chemical Weapons Act 1996

Airports (Groundhandling) Regulations 1997/2389

Police Act 1997

Bank of England Act 1998

Landmines Act 1998

Data Protection Act 1998

Human Rights Act 1998

Government of Wales Act 1998

Tax Credits Act 1999

Immigration and Asylum Act 1999

Social Security Contributions (Transfer of Functions, etc.) Act 1999

Nuclear Safeguards Act 2000

Television Licences (Disclosure of Information) Act 2000

Transport Act 2000

Utilities Act 2000

Freedom of Information Act 2000

Private Security Industry Act 2001

Anti-Terrorism, Crime and Security Act 2001

Freedom of Information (Scotland) Act 2002

Communications Act 2003

Public Audit (Wales) Act 2004

Scottish Public Services Ombudsman Act 2002 (Consequential Provisions and Modifications) Order 2004/1823

Child Trust Funds Act 2004

Commissioners for Revenue and Customs Act 2005

Education Act 2005

Public Services Ombudsman (Wales) Act 2005

Childcare Act 2006

Companies Act 2006

Equality Act 2006

National Health Service Act 2006

Wireless Telegraphy Act 2006

Statistics and Registration Act 2007

UK Borders Act 2007

Health and Social Care Act 2008

Human Fertilisation and Embryology Act 2008

Cross-border Railways Services (Working Time) Regulations 2008/1660

Criminal Justice and Immigration Act 2008

Coroners and Justice Act 2009

Cluster Munitions (Prohibitions) Act 2010

Equality Act 2010

Budget Responsibility and National Audit Act 2011

Postal Services Act 2011

Civil Aviation Act 2012

Customs Disclosure of Information and Miscellaneous Amendments Regulations 2012/1848

Legal Aid, Sentencing and Punishment of Offenders Act 2012

Welfare Reform Act 2012

Energy Act 2013

Crime and Courts Act 2013

Public Audit (Wales) Act 2013

Defence Reform Act 2014

Mesothelioma Act 2014

Criminal Justice and Courts Act 2015

Digital Economy Act 2017

Data Protection Act 2018

EUROPEAN AND INTERNATIONAL MATERIALS

European Convention on Human Rights and Fundamental Freedoms (1950)

Treaty of Rome (1957)

Recommendation 890 of the Parliamentary Assembly of the Council of Europe of 1st February 1980

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981)

Single European Act (1987)

Data Protection Directive 46/95 EC

Charter of Fundamental Rights for the European Union (2000)

Treaty of Nice (2001)

Draft Articles on State Responsibility for Internationally Wrongful Acts (2001)

Regulation (EC) No 1049/2001 of the European Parliament and of the Council of May 2001 regarding public access to European Parliament, Council and Commission documents

Treaty of Lisbon (2009)

Treaty on European Union (2009)

Treaty on the Functioning of the European Union (2009)

General Data Protection Regulation (EU) 2016/679

Directive of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (EU) 2016/680

REPORTS AND PAPERS

OECD Directorate for Scientific Affairs Group of Experts on Computer Utilisation, Computer Utilisation and the Privacy Problem: Summary of Replies to Questionnaire, 13 April 1970 DAS/SPR/70.10

Kenneth Younger, Report of the Committee on Privacy (1972)

Home Department, Computers and Privacy, Cmnd 6353 (1975)

Home Department, Computers: Safeguards for Privacy, Cmnd 6354 (1975)

Lindop, Report of the Committee, Cmnd 7341 (1978)

Recommendation of the Council of the OECD concerning guidelines governing the protection of privacy and trans-border flows of personal data (1981)

Home Office, Data Protection: The Government's Proposals for Legislation (April 1982) 1981/1982 Cmnd. 8539

Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data Com (90) 314 final – SYN 287 90/C 277/03 (27 July 1990)

Commission Communication on the protection of individuals in relation to the processing of personal data in the Community and information security (13 September 1990)

Report of the Committee on Legal Affairs and Citizens' Rights (10 February 1992)

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, COM(92) 422 final – SYN 287, 15 October 1992

Report of Permanent Representatives Committee to Internal Market Council (9 June 1994)

Rights Brought Home: The Human Rights Bill (1997), Cm 3782

Performance and Innovation Unit Report, Privacy and Data Sharing: The Way Forward for Public Services (2002)

Gus O'Donnell, Financing Britain's Future: Review of the Revenue Departments (March 2004)

HM Government, Information Sharing Vision Statement (2006)

HM Government, Transformational Government: Enabled by Technology, Annual Report (2006)

Information Commissioner's Office, What Price Privacy? (2006)

Richard Thomas and Mark Walport, Data Sharing Review Report (2008)

Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) Com(2012) 11 final (25 January 2012)

Michael Everett, The Official Secrets Acts and Official Secrecy, House of Commons Library, Briefing Paper Number CBPO7422, 17 December 2015

Law Commission, Data Sharing between Public Bodies (2014) Law Com No 351.

Law Commission, Protection of Official Data: A Consultation Paper (2017) Consultation Paper No 230.

Liberty, Abridged Briefing on the Data Protection Bill 2017: The Immigration Control Exemption (December 2017)

Open Rights Group, What is at Stake with the Immigration Exemption Legal Challenge? (3 August 2018)

ICO ANNUAL REPORTS

The Information Commissioner's Office Annual Report 2004-2005

The Information Commissioner's Office Annual Report 2005-2006

The Information Commissioner's Office Annual Report 2006-2007

The Information Commissioner's Office Annual Report 2007-2008

The Information Commissioner's Office Annual Report 2008-2009

The Information Commissioner's Office Annual Report 2009-2010

The Information Commissioner's Office Annual Report 2010-2011

The Information Commissioner's Office Annual Report 2011-2012

The Information Commissioner's Office Annual Report 2012-2013

The Information Commissioner's Office Annual Report 2013-2014

The Information Commissioner's Office Annual Report 2014-2015

NEWS ARTICLES

Kiellsson and Mendick, Journalists Who Obtain Leaked Official Material Could Be Sent to Prison Under New Proposals (The Telegraph, 11th February 2017)

Evans, Cobain, Slawson, Government Advisers Accused of 'Full-Frontal Attack' on Whistleblowers (The Guardian, 12th February 2017)

The Guardian View on Official Secrets: New Proposals Threaten Democracy (The Guardian, 12th February 2017)

Bowcott and Mason, No 10: Official Secrets Act Proposals 'Project of Previous Prime Minister' (The Guardian, 13th February 2017)

Chakrabarti, Whistleblowers Keep Us Safe. We Can't Allow Them to Be Silenced (13th February 2017)

Cobain, This Assault on Whistleblowers Exceeds Even the Draconian 1911 Act (The Guardian, 15th February 2017)