Culture of privacy : implications of data protection and freedom of information law in the UK.

CULTURE OF PRIVACY IMPLICATIONS OF DATA PROTECTION AND FREEDOM OF INFORMATION LAW IN THE UK

by

Stewart Tiltman

A Master's Thesis

Submitted in partial fulfilment of the requirements
for the award of

Master of Philosophy of Loughborough University

25 August 2003

CULTURE OF PRIVACY: IMPLICATIONS OF DATA PROTECTION AND FREEDOM OF INFORMATION LAW IN THE UK

MPhil Thesis

Stewart Tiltman

The idea of privacy begins with the concept of self-ownership, which relates in turn to the ownership of external objects, and the ontological priorities involved Privacy as a freedom to do things – private life – without undue interference, can be protected by law, but the philosophical basis for the legal means to preserve and sustain privacy requires close examination It can be shown that utilitarianism should be rejected in favour of a Kantian approach, and the importance of responsibility through moral reciprocation, rather than a facile reliance on rights, provides the soundest basis for privacy protection The NCCL (now Liberty) definition of privacy can then be ramified effectively in the light of this analysis

The legal measures to protect the privacy of data subjects, and compliance with these measures can, in turn, be examined from the same viewpoint The law sanctions some departures from the protection of privacy in the public interest regarding 'free speech' and the prevention of crime, including terrorism How matters of interest, such as these, are balanced, and the interactions of different pieces of legislation which impact on data subject privacy, are major concerns The limits of a rights-driven libertarianism with regard to interest also require exploration A detailed examination of the realities of operating the law for public authorities shows the difficulties created by the statutes, as enacted, and the implications of this for good administration

The continuous nature of privacy from the informational to the physical, and the continuum of information from the personal to the impersonal are illustrated by this analysis of the law and its practical implications An instrumental approach to rights is shown to be inadequate under these circumstances, contrasting with the cultivation of a culture of values which correctly esteem privacy and the responsibilities necessary to safeguard it Practical changes to the law which might contribute to the development of such a culture of privacy can then be identified as an outcome of the philosophical analysis and examination of the law in operation

CONTENTS

ACKNOWLEDGEMENTS

I should like to thank the following people and organisations Marion Christy, Debbie Hudson, Leon Taylor and Adam Jacobs at Melton Borough Council for their help and encouragement, Professor Paul Sturges and Professor Charles Oppenheim at Loughborough University for supervising the research, Shirley Horner at Loughborough University for assistance with the practicalities of producing the thesis, and Dr Stuart Hannabuss of Robert Gordon University, Aberdeen, and Dr James Dearnley at Loughborough University, as the examiners, for their suggestions for the final form of the thesis

Finally, I should like to thank my parents for their unstinting support

GLOSSARY OF ACRONYMS

AOL	America Online
CCTV	Close-Circuit Television
CDA 1998	Crime and Disorder Act 1998
CIPFA	Chartered Institute of Public Finance and Accountancy
DPA 1984.	Data Protection Act 1984
DPA 1998	Data Protection Act 1998
DTLR	Department of Transport, Local Government and the Regions
ECA 2000	Electronic Communications Act 2000
ECHR·	European Convention on Human Rights (Council of Europe, 1950, and as amended)
FoIA 2000	Freedom of Information Act 2000.
GCHQ	Government Communications Headquarters
HRA 1998	Human Rights Act 1998.
IRRV.	Institute of Revenues Rating and Valuation
ISP	Internet Service Provider
LGA 1972	Local Government Act 1972
LGA 2000	Local Government Act 2000
LGFA 1992	Local Government Finance Act 1992
MIT	Massachusetts Institute of Technology
NCCL	National Council for Civil Liberties (now known as Liberty)
NHS·	National Health Service
NUM.	National Union of Mineworkers
ODPM	Office of the Deputy Prime Minister
OECD	Organisation for Economic Co-operation and Development

OIC.	Office of the Information Commissioner
PFHA 1997	Protection from Harassment Act 1997.
PIDA 1998	Public Interest Disclosure Act 1998
PNC	Police National Computer
RIPA 2000	Regulation of Investigatory Powers Act 2000
UDHR	Universal Declaration of Human Rights (United Nations, 1948)
UDM	Union of Democratic Mineworkers
URL	Uniform Resource Locator

CHAPTER 1: INTRODUCTION

1.1. Context

The idea of privacy in a British legal context has been essentially a negative one – the law has sought to interfere only in specific areas of the lives of individuals Importantly, however, this has been from the point of view of the individual as a subject, rather than as a citizen, which is why the capacity for this interference has been quite far-reaching The idea of free association has often been very severely limited – as with trade union activity So has freedom of worship for religious minorities until the nineteenth century Only in 1967 did the Sexual Offences Act [1] legalise consensual sexual relations between homosexual men over 21, under considerable restrictions – equality of the age of consent only being obtained in 2000 Until recently, therefore, privacy has tended to be what was left over or left out of the law.

Rights of privacy have hitherto tended to be related to enjoyment of property and its disposal, the disposal of one's self as one's own property has tended to be reserved to the state It is interesting that the emergence of a politics of privacy – manifested in the demand for secret ballots for Parliamentary elections to prevent coercion, and religious emancipation – coincides with the arrival of Mill's *On Liberty* [2] and the explicit notion of the private space of the individual These mark in Britain the flowering of mid-Victorian liberalism It is instructive to contrast Mill's freedom to publish these ideas with Kant's much greater circumspection on the issue of privacy in the context of eighteenth century Prussia Kant [3] advances the distinction between the internal ethical realm and the external juridical one, in which the notion of the private moral space is latent, and can be inferred, but it is not until Mill that it is so strongly expressed

The rise of industrial states in the twentieth century and their technological capacity for processing information has increasingly focussed attention on the potential threat to personal privacy represented by such technology. In an American context, this led to the Privacy Act 1974 [4] In the context of Britain and Europe, the Council of Europe Convention of 1981 [5] (itself embodying many of the ideas of Sir Kenneth

Younger's Report [6] of the early 1970s) led to the Data Protection Act 1984 [7] The growth of globalism in the 1980s and the economic use of processed personal data then led to the European Data Protection Directive [8], and the creation in Britain of the Data Protection Act 1998 [9] Significantly, there is still no equivalent of an explicit Privacy Act The advent of the Human Rights Act 1998 [10], and Lord Irvine of Lairg's expressed view [11] that the courts should be creative in adding to the body of European jurisprudence a distinctly British flavour should leaven the mix Then, squaring privacy with 'the public interest' to know – freedom of information – and the requirement of national security is likely to provide further fertile ground for litigation

These changes to our legal landscape are not ideologically neutral The idea of an unbreachable personal space beyond the reach of the state is not merely anathema to the far-left, for whom it is merely bourgeois (witness the Stalinist era), but also for the political right, for whom it is a direct challenge to traditional conceptions of personhood, family and state It is a rejection of state paternalism in either form, in favour of the permanent possibility of pluralism An awareness of this dimension of political philosophy underpinning the everyday realm of law is vital, for the perceived gains and losses of different political groups as a result of changes could precipitate long-term shifts of political power Embarking on the road of data protection and human rights legislation cannot be undertaken lightly. Consequently, a proper understanding of the underlying philosophical and political concepts, and their connections and implications, is vitally important

The purpose of the first section of this work is to present a satisfactory conception of data subject privacy This will involve an examination of the idea of a private 'sphere of action' of the individual – and its limits – and of our control and ownership of information, and therefore a tapping-in to the pre-existing debate about property rights and political liberty, which has been running vigorously from the early 1970s with the publication of John Rawls' *A Theory of Justice* [12], and Robert Nozick's *Anarchy, State and Utopia* [13] Social democratic welfarism, socialism, centre-right paternalism, free-market liberalism and libertarianism have been jostling in renewed competition in the political sphere certainly since the end of the postwar economic consensus with the oil price shocks of the 1970s. The current vogue of

'communitarian' thinking is a reaction against the atomistic libertarianism precipitated by Nozick's work and its economic resonance in the work of Milton Friedman and Irving Kristol [14]

The rise of the human rights agenda – and greater protection of data subject rights – in Europe, and particularly for us in Britain, is intimately connected to this stream of political activity The philosophers Alan Ryan [15] and Thomas Nagel [16] have both been critics of the laissez-faire libertarian view espoused by Nozick, whose Utopia appears to be biased in favour of a free-market approach to political options The point to be drawn is that our legislation – the Data Protection Act 1998 and associated Acts – is not made or operated in a vacuum, it bears the political and philosophical imprimatur of those who made it This is the realm of ideas in action, the theoretical load of ontological commitments has left the laboratory conditions of the lecture theatre and become part of the real mass of the law, and part of the coinage of political debate To engage seriously with the issues of privacy and human rights means making commitments to one view rather than another, to attempt some answer to the question of what data subject privacy consists of, means taking some view or other There is no neutral commitment-free vantage point

Having drawn at the end of the first section some interim conclusions on data subject privacy, the second section – compliance – will examine how data protection law acts – or fails to act – to protect the data subject This examination will serve to test the adequacy and coherence of the vision of the politicians and their supporters who advanced the legislation

Out of this examination, conclusions about the state of our data protection laws will be sought, with the prospect of what recommendations might usefully be made to stakeholders and government with a view to improvement, or further research

1.2. Outline

To begin the analysis of privacy, what we mean by it, and what might sensibly be said about it, requires an examination of political and philosophical thought that goes beyond the familiar framework of left-right political discussion Indeed, it requires the examination of the concept of privacy, when it is usually assumed that we can simply help ourselves to it unanalysed Consequently, this constrains the choices of source literature, and the order in which these are to be understood

The study of the ontological commitments underpinning ideas about privacy – and therefore how to safeguard it – takes us beyond the conventional terms of political reference, particularly in Britain It also requires us to question otherwise unanalysed assumptions about what we mean by a 'right'

To obtain a working definition of privacy, it is necessary to return to the starting-point of essentially 'modern' arguments – Locke's conception of private property, and its origins in the private citizen's *self*-ownership The Lockean idea of private property beginning with the individual's possession of private property in the self presupposes an ontological priority of persons before property rights To make economical use of this starting-point, I have chosen to work with the collection of essays on property rights in Paul, et al , [17], against a background of Rawls, Nozick and Kant, but also Scruton [18] This involves questioning the idea of whether self-ownership is like our ownership of external objects, pointing out that there is no consensus as to what such a conception of self-ownership would be like, and criticising the view that one can think of persons in a proprietary way Rights-in-people (like privacy) might be very different from rights-in-things (like real estate)

This takes the argument to the heart of the matter regarding self-ownership, private property, and privacy, with a minimum of digression which would have lengthened the work without adding significantly to the progress of the arguments Throughout, the National Council for Civil Liberties (NCCL, now known as Liberty [19]) definition of privacy [20] is considered with the intention of ramifying it

There are, of course, tensions between the aspects of privacy being studied These arise not merely between the freedom to do something, and the freedom from something – Isaiah Berlin's positive and negative liberty [21] - which has critical implications for privacy, but also from the pull between the impulse to strive for moral objectivity and the tendency to be partial The temptation to regard liberty and equality as the same thing is to be resisted From a moral point of view, the law-abiding citizen is equal to any other law-abiding citizen, and on this basis, they should have equality of privacy, and equality of liberty to realise it But that equality is not itself liberty

Privacy is essentially a negative liberty, it is to exist as a freedom from too much power of positive rights of interference, irrespective of the democratic credentials or good intentions of those proposing the interference Notwithstanding that the behaviour of the person in private is not unlawful, privacy is unavoidably pluralistic, since it creates a space which is politically and ideologically open – it means the possibility of dissent from majority opinions, trends, fashions, beliefs This privacy, which includes that of persons as data subjects – must, if it is not to be without principle, be *reciprocal*, our equal, law-abiding citizens accord each other this freedom This entails a reciprocal responsibility to avoid its abuse, to practically obtain this, we need some conception of a general framework of law to govern it – and us – which can cross other boundaries, of race, religion, and convention Utilitarianism, as a teleological dominant-end theory, is rejected for reasons advanced by John Rawls [22], but obtaining a realistic level of consensus for a system of law requires us to also face the issue of potential conflict between impersonal moral considerations and personal commitments

This 'controlling framework' of law, and how we might actually obtain it, is the subject of the arguments considered by Thomas Nagel [23] These go to the heart of the issues about the extent to which we can pursue our own projects without considering others, to what extent we must consider others, and what limits might be placed on us, and those we elect as our agents, to obtain conformity with the law Nagel's significance is that he examines this beyond the terms of reference established by Rawls and Nozick in the 1970s, and recognises the limits to liberal

'higher-order' conceptions of impartiality in law, of the kind appealed to by human rights theorists Nagel's approach also acknowledges the conflicts of values which Berlin brought out into the open, which may have to be lived with and managed as practical politics, as these may not be amenable to any other treatment

It is from this examination of the moral underpinnings of liberty and privacy that the analysis of the adequacy of legislation and the significance of political and juridical judgement takes place It also enables the application of ideas about personal property and its likeness to 'ownership' of privacy to be viewed against the current state of the law and commonsense intuitions about privacy The first section of this work concludes by extending the National Council for Civil Liberties' definition of privacy in the light of the analysis undertaken to that point

The examination of the issues surrounding compliance with the law in the third chapter draws chiefly on the legislation itself, commentaries on its jurisprudence, and the case law

Having unpacked many of the arguments and ideas about privacy, and the extent to which the law does – or does not – secure it, the fourth chapter draws out the key elements of privacy and their significance One of the key sources here is Francesca Klug [24], as someone closely linked to the project to create the Human Rights Act 1998 There is also a survey of the policy documents on where the Labour Government (at the time of writing) wishes to go with regard to the use of data The fifth, and final, chapter draws together the arguments and sets out conclusions and recommendations arising out of these conclusions

1.3. Aims and method.

The aims of this thesis can be set out in the following way

- An examination of the nature and legal status of privacy
- An analysis leading to a working definition of privacy
- An enquiry into the ontological commitments involved in the concept of privacy
- An examination of how the analysis of privacy informs the study of compliance within the law.
- Advancing a critique of the libertarian, rights-based approach to data subject privacy and public interest
- Making recommendations with a view to improving the effectiveness of information law, and pointing to the creation of a value-culture of privacy

The method employed in writing this thesis may be set out as follows

- A close examination of philosophical literature relating to the theory of ownership, privacy, interest and ethics, relating to the individual
- A detailed examination of the legislation and commentaries by leading practitioners in data protection, freedom of information, and human rights
- A critical analysis of the material against the background of the real-world experience of public authority implementation and operation of the law
- Critical reflection upon the evidence, analysis and experience to derive conclusions and recommendations for possible actions

CHAPTER 2: PRIVACY

2.1. Rights

In setting out an adequate working definition of privacy we need to be aware that we are making commitments to other conceptual or material entities. It is intended in this study that these ontological commitments should be uncovered and analysed as part of the process of setting out what could sensibly and defendably be called privacy

2.1.1. The liberty of privacy

In its submission to the Younger Committee in 1972, the then National Council for Civil Liberties (NCCL) [1] presented a draft definition of what it considered to be the right of privacy.

(a) solitude – being his right to have his physical senses unmolested in any private place
(b) intimacy – being his right to enjoy in any private place the close familiarity of his family, work group or social group.
(c) anonymity – being his right to prevent undue publicity of himself
(d) reserve – being his right to prevent psychological investigation on his mind or brain
(e) privacy of his personal information – being his right to prevent the reading, copying or recording of any information kept by him or by any other person which expressly or by necessary implication refers to him

(It is to be understood that 'he' throughout should be read as also applying equally to 'she')

It is interesting to see what this definition leaves out Solitude is not merely, it would seem, a matter of not having one's senses – or sensibilities – molested (which attempts to capture the combination of assault and offence) Rather, a certain amount of solitude is a freedom from the social pressure of others, a freedom to be apart from others when one wishes it Reserve, also, would seem to need to include a sense of physical or psychological freedom from scrutiny – the NCCL definition, if it is relying on the laws relating to assault to cover this, rather seems to accept either a

version of dualism about minds and bodies – which would be regarded as untenable – or not to take seriously enough the importance of one's own physical space

Alan Ryan [2] points out that self ownership is a starting point often used by libertarians to launch arguments about privacy and property rights, starting with Locke's notion of private property beginning with the individual's prior possession of private property "in his own person" [3] As Ryan asks, just how is this like our ownership of external objects? Locke's argument requires the prior existence of autonomous selves before we can consider the issue of ownership of property This introduces an ontological priority that persons must be recognised in a moral universe of discourse before property rights, without human agents and human agency, the institution of human property is senseless

Furthermore, as Ryan asserts, there is no consensus as to what such a conception of self-property would be like – the very different standpoints presented by Thompson and Finnis on abortion highlight this quite dramatically [4] Along Kantian lines, we are drawn into governing ourselves in societies with legal institutions and rules of justice governing our external conduct creating a political order without compromising our internal freedom

because there are some things that cannot be made objects of a proprietary relationship, namely those things closest to our personality [5]

More pointedly still, Ryan maintains that Hegel shows that the idea of being able to part with all aspects of our personality is incoherent, since we could not do so without eliminating just that feature of ourselves on which that idea depends

To be cashable, privacy requires autonomy, and to be a coherent idea, autonomy requires moral agency, and this requires rational moral agents, who are capable of being autonomous and agentive Privacy, then, as it is discussed by politicians and lawyers, comes prepacked with ontological commitments But this is not all the commitments, Ryan criticises Nozick's view as being inadequate, since there is no consideration by Nozick that a proprietary way of thinking might be inappropriate Nozick seems to assume that if we do not own ourselves, then simply some other(s)

must have at least part-ownership of us The libertarians – certainly of the Nozickian kind – do not seem to have considered that rights-in-people (like privacy) might be very different from rights-to-things (like real estate)

Munzer [6] sheds further light on this issue, his argument revolves around the idea of a market in body parts for medical use The Nozickian position would tend to suggest that we could straightforwardly dispose of parts of ourselves as we see fit, rather like trading in spare car parts Munzer uses some arguments from Radin that connections exist between property and personhood, to achieve and sustain personhood , human beings need some control over resources in the external environment in the form of property rights, which are in 2 classes

(1) fungible property rights – for property regarded instrumentally
(2) personal property rights – property 'for personhood'

However, Radin does not draw a clear line between alienable and inalienable or between persons and things, which weakens her version of the argument, Munzer therefore refers back to a Kantian starting point Persons have *dignity*

Dignity is an attribute of persons as ends in themselves [7]

Dignity and personhood are to be understood as belonging to every rational person with a will, as members of a moral community, a Kantian commonwealth Hence we are all equally moral 'players' Body and self are the *person*, and for its continuation, those body parts necessary for its normal biological function naturally have a different status from other body parts – like hair – that do not. (There is a further contrast for Munzer with donations which are given without a financial market transaction, a freely given gift). Selling body parts – those of this necessary kind – is objectionable, because it puts us on a slippery slope, since it compromises the status of a person as not merely a thing, which threatens the personhood of persons We are worth more than the sum of the market value of our body parts There is a danger that valuations on compensation for injury in tort encourage this kind of depersonalisation Ultimately, we have to question whether self-ownership is a coherent idea The notion of the self and its body is misleading because it creates – and rather relies on –

dualism of an at least sub-Cartesian kind, it would be better to speak of *persons*, since it is this dualism which tempts us to view bodies as merely things, setting us up to step onto the slippery slope. In the penumbra of the person there is personal property, which naturally then falls out as that property (those things) a person has for the continuation of that person and the promotion of what Bernard Williams [8] calls *projects* Only at this point do we then reach outward from the person far enough to the realm of fungible (or instrumental) property

We seem to have come a long way from talking about privacy, but the point is how privacy is bound up with the control by the self of one's own body, its means of sustenance (food, shelter, work, etc) and its ultimate disposal (wills, funerals, transfer of associated goods) The relationship between the self and its physical, material embodiment is not like that of any other property relationship, the Nozickian approach is simply misleading The Nozickian view is too instrumental, and fails to capture the sense – and essence – of dignity Bound up with the notion of control belonging with privacy is control of information about the self which if misused could lead to unwanted attention and risks to personal security and the vital interests of the self, with concomitant restrictions on freedom of action How this *autonomy* - this freedom of action – which is necessary to ensure one's privacy is to be maintained will be explored once the historical circumstances leading to present day concerns have been examined, supplying the context

Part of the argument about the appropriate means of safeguarding privacy depends on what view we take of rights more broadly Lord Irvine of Lairg [9] refers to a dichotomy between *constitutionalist* and *sovereigntist* approaches to this issue , in the context of human rights generally As this applies to privacy, it is instructive to distinguish between the traditional English-speaking legal view, which it is useful to characterise as *organic* privacy, and the view associated with Lord Irvine's constitutionalists, which might be termed *formal* privacy Irvine points out, not without irony for a man ostensibly of the left, that collective democracy (and its corollary, parliamentary sovereignty) have too often failed to protect individual liberty. 'Freedom under the law' can deny or defeat basic human rights – notably from our point of view, privacy

There is, though, a deeper philosophical concern which is touched upon here, which shows the inhuman scale of this collectivity Scruton [10] emphasises the conservative form of this collectivity, which is quite capable of being a 'despotism of the majority' [11] But even Irvine [12] says

Like Parliament, Congress also represents an elected legislature giving effect to the popular will

This *geist* of the popular will is a most dangerous Rousseauian abstraction The most we can treat ourselves to in political-ontological terms is the product of the 'sum-over-electoral-histories' that is the outcome of an election Anything else is a metaphysical conceit This is a concern because privacy and individual rights are vulnerable to conceits of the 'greater good' which smuggle in notions of the 'general will' We must be vigilant against the temptation to prefer reified social abstractions over real people

The historical trajectory of the notion of privacy is illuminating Porter [13] in his study of the eighteenth century emphasises the deregulated nature of the world of pre-industrial Britain, where privacy meant very much a right to dispose of one's own property as one saw fit (provided that one *had* property). The notion of privacy extending to 'personal' issues and confidences existed only in the realm of gentlemen's agreements It is salutary to note that attempts at the end of the eighteenth century to introduce central registration of births, marriages and deaths, and censuses, were not successful, as an interference with organic liberty, notably as a contrast to the foreign centralised rationality of revolutionary France (The census was finally admitted as necessary as part of the Napoleonic war effort) The problem with this organic liberty and privacy is its vulnerability to capricious interference In a predominantly rural society, there is the mentality of the village-sized community, where everyone's business is often soon known Lawmaking contained nothing of the modern idea of a programme for a term of governmental office, since there were no modern democratic pressures acting as 'drivers' on the process. In these conditions, privacy in the sense of personal freedom from others and their attentions does not really exist in law, so much as in the interstices of life left alone by the law For the bulk of society, living conditions meant little privacy in this sense – either because of the close-knit social nature of rural society or the crowded conditions of the first

urban areas like London A further element of capriciousness was added by the activities of 'mobs' in this period

The first indications, however, of the wave of change to be brought in by industrialisation can be noted with the founding, in 1775, of the Sunday Observance Society, a shift towards the more puritan middle-class values reaching their apogee in the nineteenth and early twentieth centuries As Porter remarks [14]

Respectability – a word first used in 1785 – was beginning its meteoric career

By the late 1790s the beginnings of factory discipline, with long hours and no physical privacy, plus the effects of the tough legislation suspending traditional organic liberties due to the Napoleonic wars, meant the end of pre-industrial interstitial freedom for many This continued throughout the pre-Reform Act period, as with the Peterloo massacre and its anti-Chartist aftermath But the effects of industrialisation were driving up the pressure for reform of the political arrangements of Britain The first Reform Act of 1832 and reform of the old corporations beginning in 1835, with the Municipal Reform Act and the Poor Law reform of 1834, mark the advent of the new capitalistic, bureaucratic state, and the beginning of the end for the traditional society based on older patterns of land ownership

But these changes, at first, had little effect in improving privacy for the majority of urban dwellers, overcrowded and poor What was happening was the emergence of privacy issues for the middle classes – respectability, the importance of family life as a respite from work, and a growing dissatisfaction with 'mobby' elections , which led in 1872 to the Gladstone government introducing the Secret Ballot Act, with the concomitant gain in political privacy, and the end of election-time intimidation This marks a period of transition to greater rationalisation and formalism, away from the organicism of the old legal and parliamentary arrangements, highlighted by the Selborne reforms of 1872-1874 Another aspect of respectability was religious toleration – leading to the 'privatisation' of belief, and the growth of personal varieties of Christianity, and of secularism While the greater regulation of life seems like interference to us, because it was not balanced by any statutory extension of

privacy, it was welcomed by many in the mid-Victorian period as ushering out the violence and lawlessness of the pre-Reform era

Rationality and respectability were shifting the balance from organicism towards formalism Parliamentary reforms like the 1884-5 extension of the franchise and the greater use of single-member constituencies, and the creation in 1888 of County Councils show the thoroughness of the moves to rationalisation of government But also, the rise of 'interfering' legislation – mental health detainment, the sweeping criminalisation of male homosexuality in s11 of the Criminal Law Amendment Act of 1885 – reveal that the centralising tendencies of a rationalised state were being exercised

The tension between political and administrative rationality and abuse of its power was captured by Mill in 1859 in *On Liberty* (even before the reforms of the 1870s and 1880s) Freedom, and a private life – the freedom to pursue one's own ideas and inclinations without harm to others – Mill saw as a prerequisite of a civilised society, and essential for establishing ethical and political truth Also, that this would have to be freedom from what could, under democratic rule, become a tyranny of the majority The rise of the modern state, with the persistence of the attachment to concepts of personal freedom, and the rise of densely populated urban landscapes focuses privacy into the form the word connotes today, with its emphasis on freedom from others, and from their judgements

It was against the background of the attempted remedy for the Criminal Law Amendment Act 1885, in the form of the Report of the Committee on Homosexual Offences and Prostitution – generally known as the Wolfenden Report [15] – that the post-Second World War attempts at a British privacy law were first launched

The Wolfenden Report was published on the 5 September 1957, and contains the following statement of principle regarding homosexual behaviour between consenting adults in private

> there must remain a realm of private morality and immorality which is, in brief and crude terms, not the law's business [16]

This is an instantiation of a general maxim, acknowledged at the time, of Mill's liberal doctrine in *On Liberty* [17], and this maxim may further be seen as deriving from a Kantian distinction between juridical duties, that may be imposed by external juridical laws, and ethical duties, which must be adopted voluntarily by the moral agent [18] This private realm is bounded by law, but was no longer to be subject to the interference of the law, on the grounds of consent

Between the 1960 and 1962 votes on Wolfenden's recommendations in Parliament (the proposals were rejected on both occasions), Lord Mancroft introduced a Private Members' Bill regarding privacy in 1961 [19] which was also unsuccessful A further Private Member's Bill was introduced in 1970 by the Labour MP, Brian Walden, in response to which the Younger Committee was set up by the Government [20]

(The principle of consenting homosexual relations in private over the age of 21 was finally passed by Parliament on 4 July 1967, receiving Royal Assent on 27 July 1967, as the result of a Private Member's Bill launched by the Labour MP, Leo Abse, and lobbying in the House of Lords by Lord Arran)

The Younger Committee's Report was published in 1972 [21] It concluded against establishing a general law on privacy, but made some specific recommendations regarding privacy in relation to information, including credit rating agencies, private detectives, and computers. The last of these issues precipitated the setting-up of the Lindop Committee [22] – which reported in 1978 – to obtain detailed advice on the establishment and composition of a Data Protection Authority , but these proposals were, like Younger's, not acted upon It was the Council of Europe Convention of 1981 [23] which drew on the Younger Report, that finally provided the impetus for the Data Protection Act 1984 This Act was, however, concerned only with computerised records The issue of paper records was addressed later, by the Access to Personal Files Act 1987

The focus shifted back to a more general concern with privacy in the late 1980s with regard to press intrusion into private lives Private Member's Bills were introduced into the House of Commons in the Parliamentary session of 1987/88 by the Conservative MP, William Cash, and in the session of 1988/89 by the Conservative

MP, John Browne. The second of these Bills – the more successful of the two – was withdrawn at Report stage with the Government's announcement of a committee to be chaired by David Calcutt QC to investigate the protection of individual privacy from press intrusion

The Calcutt Report [24] concluded that there should not be a statutory tort of infringement of privacy, and out of the Report, self-regulation of the press via the Press Complaints Commission and the Press Complaints Tribunal emerged as primary means of dealing with privacy intrusions Two years after the Report, the now Sir David Calcutt QC was asked to consider if this self-regulation had worked he concluded that it had not, and recommended that the Government should consider further the matter of a new tort of infringement of privacy [25] Out of these considerations, arose the *Infringement of Privacy* Consultation Paper [26]

The notions of private space and quiet enjoyment of one's own property have become a general requirement The sovereigntist view of the rights of the parliamentary state over the individual has finally found a challenge in a greater respect for the rights of the individual The inadequacy of the organic approach to protect these has not merely been a feature of British society – twentieth century history has forced the growth of international mechanisms to safeguard some of the essential features of privacy Formalism – the making of laws designed to promote the protection of privacy – has overridden the organic approach

Experience would tend to suggest that organic privacy is not strong enough to thrive, only those with power and influence can significantly benefit from it, often at the expense of others A democratic age leads to pressure to extend privacy to everyone as a basic entitlement – a *right*. Legislation, then, seems inescapable, since – as we stressed earlier – freedom to actualise privacy – *autonomy* – is the key that unlocks privacy We therefore must have the legal entitlement of control over our own affairs, and this entails a control over the disposal of information about ourselves and our personal commitments and projects, to have everything glaringly public would denature our personal commitments, not least by warping our ability to act freely and without unwelcome attention

There must, therefore, be a freedom to exercise the right of privacy, to be meaningful, it must be cashable, and this then entails a degree of material freedom of action to exercise it This is why autonomy of the individual has been difficult to separate from the notion of privacy in itself Old people in nursing homes, for example, are private citizens, but they may well lack the material autonomy to exercise any theoretical privacy they might otherwise be considered to have Their right of privacy is rendered empty It fails on the grounds of sufficient autonomy, or of solitude Loss of anonymity also has implications for autonomy, since the freedom to act in pursuit of one's own projects without undue restriction or impediment is lost.

A commitment to privacy is, then, a commitment to personal autonomy This personal autonomy is dependent upon consensual control of not merely our bodies but also of our material property, and information about ourselves, and like those essential Kantian material parts of ourselves, *information* about ourselves is not something we can dispose of without thought The consequences of so doing could be just as life-threatening as the giving up of body parts Furthermore, this may apply to associations of persons, do combinations of natural persons have status as agents with rights – *legal persons* – or do rights only attach to the individuals themselves?

The current data protection legislation has been construed to be compliant with the respect for private life and freedom of information contained in Articles 8 and 10 of the ECHR Douwe Korff [27] quotes the Explanatory Memorandum to the OECD Guidelines

> Some countries consider that the protection required for data relating to individuals may be similar in nature to the protection required for data relating to business enterprises, associations and groups which may or may not possess legal personality

It remains open under Article 3(2) of the Council of Europe Convention [28] to recognise the legitimacy of extending data protection to legal persons

This must require an answer, then, to the question of whether the very notion of legal personality for organisations actually makes sense Organisations must have certain legal rights to be able to function at all Some of these are those which we would

accord to natural persons Autonomy – freedom of action, insofar as this does not adversely affect others, is clearly necessary They have rights over property in the form of assets, and a right of confidentiality over their information They must also have the right of a fair hearing, both as organisations operating amongst other organisations, but also because the natural persons working for them need to be able to actually perform their duties without unreasonable hindrance

Interestingly, a private organisation has been able to exercise this right in a British context; Nicholas Dobson [29] points to the case of *County Properties Ltd v The Scottish Ministers* where it was concluded that County Properties had its human rights abused under Article 6 of the ECHR via the HRA 1998 County Properties Ltd have had the benefit of a law designed for natural person 'victims'. This appears to teeter on the brink of admitting the existence of the equality of legal personality in UK law But the right to a fair hearing is the sort of thing which an organisation – or its individual human representatives – could reasonably be said to have, since it seems to be the kind of rule which would apply to persons under any description, either as individuals or as agents of an organisation It certainly does not seem necessary to admit the existence of the equality of natural and legal personality to secure practical rights for organisations, the catalytic effect of the HRA 1998 on common law seems to be creating a climate in which tortious remedies are quickly becoming available Such a route would also preserve the special status of natural persons The County Properties judgement does not yet seem to have crossed the line, even if it has come up to meet it

German law takes the view that rights revolve around the right to respect of one's personality, *das allgemeine Personlichkeitsrecht*, there is no organisational equivalent of *das allgemeine Organisationlichkeitsrecht*, no right to respect of 'organisationality' It would seem that any personality an organisation has – its ethos – derives from the natural persons who work in it Ethos, like the rest of the organisation, supervenes on the human Even if we call the organisation a legal person, it has no natural personhood, and could not experience privacy, only confidentiality For example, Texaco has no private life – it doesn't go home to its family at the end of a working day, only its workforce does – but it does have property rights since Texaco can have assets Confidentiality is the business

equivalent of the privacy of the natural person's data subject information, confidential information is not necessarily personal information Organisations are extensions of natural persons, and do not ultimately exist without them It is interesting to consider that the philosophical refusal in postwar Germany to accept the equality of natural and legal persons is a deliberate refusal to accept the claims of parties or groups over individuals, and a bulwark against the romantic idealism that led to Nazism placing party and state over people. Organisations are therefore derived entities, and not of the same category or type as natural persons, and this is probably a good reason for attaching fundamental rights only to individual, natural persons The effects of s 2 of the HRA 1998 and the possibility of admitting the equality of legal personality into English law will need to be watched closely, it would be a disturbing irony if something intended to protect individuals against the misuse of state power actually encouraged the power of organisations over people

The issues of the rights of individual privacy and the rights of organisations meet in determining the scope of individual privacy in the workplace, and this brings us back to the matter of the integrity of the person and ownership. Irrespective of the existence of the status of legal persons, organisations will be considered to have rights over the use of their assets, including their workplace facilities At the same time, individuals working in these facilities cannot be asked to give up their personhood There must then be some accommodation between the individual and the organisation

The NCCL definition of privacy includes solitude and anonymity These are important in the workplace – as anywhere else – in maintaining the integrity and dignity of the individual. But the issue is one of whether the behaviour of a person in a private place is appropriate to a workplace, which is essentially a *public* place Furthermore, the space in which all this is taking place is not like an open air space for leisure purposes The space belongs to the organisation, and the space – and the individual – is there for a particular purpose or range of purposes The individual is there in a particular guise or *role*

Individual X occupies a workstation, say, in virtue of being postholder Y, not individual X, Z could just as easily be postholder Y X exists in relation to the organisation via being postholder Y The desks, computers, cupboards and files are all

the property of the organisation – assets – and are used by X in the persona of postholder Y The post Y is itself part of the organisation X's briefcase, by contrast, belongs to X in virtue of X being X, and is a space owned by X Data manipulated by X belong to the organisation, and are governed by the rules of the organisation and any laws to which the organisation is subject as a data controller X, as an adult bound by a valid contract of employment, retains certain fundamental rights, but also, as a contracting adult, has placed himself (or herself) under a duty to perform certain tasks and may not use the organisation's property (assets) for purposes beyond those authorised by the organisation. Ultimately, the workplace is not a home, and its responsibilities require the adoption of a role which binds the capacity for freedom of action, entailing restrictions on autonomy

Our liberty of privacy is thus subject to compromises in our interactions with others Our personal relations can require the most intimate of compromises, while our employment often requires the channelling of our autonomous action toward goals shared with others, even where this can be at some inconvenience to our own personal interests and projects

2.1.2. Negative and positive liberty

One of the dichotomies we have touched upon is that between an informal, organic privacy and a formal, legalistically conceived and protected privacy If we promote the notion of privacy through legislation, as with the HRA 1998, and the DPA 1998, to what else might this commit us? Even with the backing of legal prescription, the kind of privacy we are seeking to protect would appear to be the kind which Berlin [30] characterises as *negative* liberty, it is within that area where the subject should be left to do or to be what they are able to do or to be without interference This kind of liberty is subject to the practical restrictions of laws to protect others, the liberty of some, therefore, depends upon the restraint of others (This reciprocal aspect of liberty – and therefore of privacy – will be returned to in 2 2) Berlin then asks – as we have – what is freedom (to do as one pleases in matters concerning ourselves) to those who can make no use of it? Political rights and protection against an overmighty state mock the very poor, whose pressing material needs would seem to demand attention before the apparent niceties of political liberty If individual liberty – including our

liberty of privacy – is an ultimate end for human beings it is so for all human beings, we need equality of liberty But Berlin makes an observation then which tends to be glossed over by many liberal thinkers.

If the liberty of myself or my class or nation depends on the misery of a number of other human beings, the system which promotes this is unjust and immoral But if I curtail or lose my freedom in order to lessen the shame of such inequality, and do not thereby materially increase the individual liberty of others, an absolute loss of liberty occurs [31]

Very simply equality is not liberty Furthermore, the Millian conception of negative liberty is unusual, a post-Enlightenment product, not appearing in any of the classical or ancient civilisations Still further, Berlin signifies that it is not dependent on democracy, such a private space could be compatible with an otherwise autocratic or dictatorial government. It would be possible for a strictly majoritarian government to use its majority power to be more ruthless in smothering minorities

Within this private space – and over one's own life and property – one naturally wishes to be master, and this has tended to mean a rational master, even if only narrowly, instrumentally so This wish, Berlin suggests, is the basis of the impulse to establish *positive* liberty Establishing this mastery seems uncontroversial so far as it merely involves each rational person in determining their own affairs according to their own pattern This would, for instance, make the notion of information about the self very much a matter for control by the self, as part of our being able to be master over our own affairs The problem really begins where the *real* self that seeks mastery is identified with something else – like Rousseau's 'general will'. Governing elites with the power to harness and influence the popular will are subject to the teleological temptation to make individuals free according to someone else's pattern, with the populist general will as an amplifier to drown out the sounds of dissent This is the strongest form of political paternalism, manifested, for example, in Stalinist or fascist indoctrination As Berlin remarks.

Those who believed in freedom as rational self-direction were bound, sooner or later, to consider how this was to be applied not merely to a man's inner life, but to his relations with other members of his society [32]

The danger of rationalism is its tendency to seek for one true plan for society. Paternalism is despotic because it is

an insult to my conception of myself as a human being [33]

This may even be the case where the paternalism is well-intentioned, which is why people might sometimes prefer organic societies lacking in formal respect for legal rights, but where familiar faces and surroundings mean that one is treated as a human being, where institutional relationships are on a human scale This is what Berlin calls the search for *status*, and this status – solidarity, fraternity, equality – is not the same as liberty, but is one of the things that gives life value, and is bound up with the human requirement of belonging However, the realisation of this belonging after our own manner and those like us may manifest itself as nationalism This liberty of belonging as we choose can itself become tyrannical if it is used to impose our (group's) conception of belonging on others Positive (socially-conceived) liberty can easily erode negative (individualistically-conceived) liberty The issue of authority and power then becomes not so much *who* wields power (the traditional question of politics between autocracies versus democracies, for example) as *how much* power can be entrusted to any set of hands whatever

This is where we came in The ECHR – via the HRA 1998, and the DPA 1998 – restrict the agencies of the state and other organisations from merely disposing of information about data subjects without reference to the views, projects, intentions and wishes of the data subjects themselves Limits *have* been placed on how much power can be entrusted to any set of hands whatever Also, we have rejected a positively-liberal empowerment of groups of like-minded individuals by rejecting the 'social embodiment' arguments of countries like Italy, in its support for legal personality, in favour of a German-style restriction to natural persons, to this extent, negative liberty is bolstered by law More than this, political pluralism is embodied fundamentally in the ECHR-HRA regime, and Article 8 is the corollary of this for individual privacy. But there is in Berlin's essay a warning against a glib utilitarianism in handling these values

To assume that all values can be graded on one scale, so that it is a mere matter of inspection to determine the highest, seems to me to falsify our knowledge that men are free agents [34]

Pluralism is not to be seen as merely a matter of different utilitarian 'happinesses' which can be embraced by some attempt at a reconciliation of these happinesses by a second-order 'meta'-happiness, Berlin wishes us to seriously consider that plural values could really be incommensurable, resistant to reductive sleights-of-hand Utilitarianism, while not unattractive, is incorrigibly teleological The legal framework which we use to contain this diversity of people and projects may be durable and formalisable, but it is provisional Berlin suggests that the liberal values upon which it is based may be less than eternal

Principles are not less sacred because their duration cannot be guaranteed [35]

Berlin seems to have given only two cheers for rationality, but the operation of value pluralism will need some legal framework, and this framework, if it is to command public support, must be seen to be reasonable If the law is not to appear capricious, it needs to be rational Rationality seems to be a very deeply ingrained commitment or presupposition which we cannot dispense with The law confers its rights on our private data subject in a manner which is amenable to reason However, the constraints of the law are reciprocal, since there is no freedom to do just as we like without reference to the rights of other private subjects Also, for data subjects who also work for data controllers, those data subjects must act to *confer* rights on others as a specific legal obligation, rather than just as a general legal or moral one
Even privacy, then, is not unlimited Equality of privacy for all data subjects means practical limits on what each might do with their personal space in pursuit of their own projects, in that where those involve others – or information about others – equality of treatment means equal restrictions on otherwise complete liberty of action Liberty might thus be diminished in some instances, but it would seem to make it socially broader-based Arising out of this liberal idea of equality, is the question of how equality might actually be obtained Both the HRA 1998 and the DPA 1998 confer rights, but the way in which these rights are to be secured equally between individuals is largely tacitly assumed The key would seem to be that the rights and constraints on each are *reciprocal*

2.2. Responsibilities

Our liberty – and our liberty of privacy – cannot be entirely unlimited, simply because we live in a world where there are others who also have similar moral and legal claims as ourselves Interestingly, this is specifically acknowledged within the framework of the HRA 1998, Home Office guidance to the public makes this clear

> In a democratic society everyone has rights Your rights come first, but so do everyone else's So we all have to accept some limits on our rights in order to make sure others are treated fairly [36]

To what then does this acknowledgement of responsibility commit us?

2.2.1. Reciprocity

In the discussion of Berlin's ideas of negative and positive liberty, it was suggested that if liberty – and privacy – were ultimate ends for human beings, they were so for all human beings This yielded up a basic requirement for the notion of equality, but did so in a way which promoted a teleological view of liberty (analogous to utilitarian happiness) as a dominant end Obtaining equality this way looks therefore like a surrender to teleological temptation, but at the same time, liberty – and privacy – are desirable moral and political goods The point is that liberty and privacy are not teleological purposes, rather, they are desirable to make other things possible – like Williamsian projects Liberty and privacy are heterogeneous since their contents vary from individual to individual, and the values of these contents cannot be commensurated on a single scale, as Berlin has already suggested

In outlining a theory of liberty – and therefore of the importance of privacy for data subjects – we are faced with a fundamental choice as to how we set this up Teleological theories lead to one dominant-end conception, like happiness The oddness of this Rawls [37] makes abundantly clear

> The extreme nature of dominant-end views is often concealed by the vagueness and ambiguity of the end proposed And certainly when the dominant end is clearly specified as attaining some objective goal such as political power or material wealth, the underlying fanaticism and inhumanity is manifest

Human good is heterogeneous because the aims of the self are heterogeneous Although to subordinate all our aims to one end does not strictly speaking violate the principles of rational choice (not the counting principles anyway), it still strikes us as irrational, or more likely as mad The self is disfigured and put in the service of one of its ends for the sake of system [38]

And further

The weakness of hedonism reflects the impossibility of defining an appropriate definite end to be maximized And this suggests that the structure of teleological doctrines is radically misconceived from the start they relate the right and the good the wrong way We should not attempt to give form to our life by first looking to the good independently defined It is not our aims that primarily reveal our nature but rather the principles that we would acknowledge to govern the background conditions under which these aims are to be formed and the manner in which they are to be pursued For the self is prior to the ends which are affirmed by it, even a dominant end must be chosen from among numerous possibilities [39]

Teleological theories therefore exhibit a fundamental failure of ontological priority, since persons are prior to values But we want to be able to say that there is an underlying equality between the moral statuses of individuals with regard to their liberties We need therefore a tenable account of the *universalisability* of rules we make about equality of liberty and privacy For the whole idea of having laws regarding data privacy is that they should apply equally to all data subjects We have also, in embarking on this ontological shift of priority, given up the dominant-end obsession and distortion and moved to talking about rules and their formation The conferring nature of rules also makes each right a duty, since there is always an other-directed aspect to every right, that we must accord others the same rights we enjoy, yielding reciprocity.

Once again there is the limiting of pure freedom of action in the service of the rights of others, but this does not relieve the tension revealed by Berlin between plural values Moreover we cannot avoid dealing with the surrender of some autonomy in the service of the institution of law in the pooling of the sovereignty of individuals in society An attempt to address these matters is presented by Nagel [40] in his exploration of the relationship between personal and impersonal moral standpoints What Nagel calls the Kantian standpoint he wishes to work from he characterises thus·

it attempts to see things simultaneously from each individual's point of view and arrive at a form of motivation which they can all share, instead of simply replacing the individual perspectives by an impersonal one reached by stepping outside them all – as happens in the attitude of pure impartial benevolence [41]

It could not be sufficient, Nagel maintains, to either leave the two standpoints to fight it out or reach some kind of accommodation within each individual, there needs to be law There is, though, danger in the detail of how this Kantian development of the impersonal standpoint is to be set up Nagel characterises the idea of what (he thinks) is reasonable

It is what I can affirm that anyone ought to do in my place, and what therefore everyone ought to agree that it is right for me to do *as things are* [42]

This appears much too narrow – the attempt at reciprocity is very grudging, and it takes insufficient account of the impersonal view Worse, the second part does not follow clearly from the first There needs to be a rider as to what I would do in someone else's place Setting the matter up as Nagel has, there is a danger that narrowing the sympathies of the self at the beginning in this formulation will constrain the development of the argument in a way that could be seen as tendentious Nagel admits the real significance of the impersonal standpoint

I believe that if people's lives matter impersonally at all, they matter hugely They matter so much, in fact, that the recognition of it is hard to bear, and most of us engage in some degree of suppression of the impersonal standpoint in order to avoid facing our pathetic failure to meet its claims [43]

Solutions to this problem need to

engage the impersonal allegiance of individuals while at the same time permitting their personal motives some free play in the conduct demanded by the system [44]

Utopian solutions are always prone to come to grief in handling the realm of the personal, the reason why, as Rawls says, the theory of the right must come before the theory of the good, so that we are not to have a theory torn to pieces by a competition of various 'goods' Also there is the risk of trying, as TS Eliot [45] once remarked, to

invent a system so perfect that no-one has to be good, which would be the suspicion with a utilitarian felicific calculus

Nagel identifies that a legitimate moral view is going to be that which can produce not unanimity about everything, but about the 'controlling framework', which is as much as Berlin's analysis suggests that we might obtain The accommodation of the personal standpoint requires Nagel asserts, a theory of *agent-relative* reasons for action,

> reasons specified by universal principles which nevertheless refer ineliminably to features or circumstances of the agent for whom they are reasons [46]

These are to contrast with *agent-neutral* reasons, which are to depend upon those things which everyone should value independently of any relation to the self The agent-relative reasons cannot involve a person in doing something wilfully contrary to reason – anti-rational – or which seeks to gain some advantage by exploiting another, by treating them as a means rather than an end The point thus being that, any rule which involves a person in choices which are *not in principle* universalisable is ruled out at the start Nagel's questions at this point are – how can we determine in relation to a particular maxim whether or not it can or cannot be willed to be a universal law? And what would it mean to be able to conceive of it as such but not able to will it as such? Hare [47] eventually takes utilitarianism as the solution, by collapsing deontology and teleology, with utilitarianism as the only rational mechanism for resolving conflicts of interest, but we have already rejected utilitarianism on teleological grounds, one might just as well suggest that rule-utilitarianism collapses into deontology

Nagel, however, intends to advance an ideal of 'universal acceptability' as an alternative to the pure dominance of the impersonal standpoint, and to utilitarianism There are two general judgements which, for the pure impersonal standpoint, there are no easy ways of reconciling·

(1) Everyone's life is equally important
(2) Everyone has his own life to lead

Nagel rules out moral justification by a reason that simply derives from what someone already wants. It would also be far from preferable if morality were then to be reduced to a balance-of-power-like system of bargaining, like politics

> We should not be satisfied with a mere bargain, if the process that leads to it does not confer on it a moral validity that makes the result immune to further moral criticism [48]

The suspicion that Nagel voices is that there may be no general principles governing both agent-relative (personal) and agent-neutral (impartial) ones which are acceptable from all points of view in the light of their consequences in all probable conditions Kantian unanimity is a stiff challenge that might not be met Any solution must carry the weight of political legitimacy, which is why there must be a social – that is, legal – version of the individual rule for conduct Or as Nagel puts it

> Principles of individual conduct are not enough The world has to cooperate [49]

How this is to be squared with the personal Nagel himself indicates

> If we wish to let our personal point of view affect our attitudes in a way that is not objectionable, it must be in accordance with conditions which we judge would be reasonable for anyone [50]

The limits to equality arise out of the personal or agent-relative area. The supervenience of society upon the individuals who comprise it is the mechanism which makes the egalitarianism of institutions compromisingly dependent upon the anti-egalitarian partiality of the individuals out of which they are built This partiality of individuals or groups makes for the likelihood of the incommensurability of values, and a failure to even agree a controlling framework is what frustrates the growth of democracy, or as the history of the 1930s shows, causes the failure of existing democracies Only the successful practical exercise of reciprocity can ensure that the pursuit of liberty – and therefore privacy – by a number of individuals is not mutually inconsistent

Failure to agree to a controlling framework, such as a bill of human rights, or even a robust system of common law, means that privacy would only be protected patchily

But also there needs to be a widespread acceptance of the principles of privacy – and therefore of the need to protect data, we may have a legal framework in place, but there needs to be a resolve to maintain and enforce it The failure of Canada's 1960 attempt at a human rights law is an example of this failure to obtain acceptance of such a controlling framework, particularly from those powerful interests in society who can make a difference to the successful adoption of such legislation Rights may be brought home, but their welcome once there is not guaranteed

We need to consider, then, what limits there are to the *tolerance* of diversity, since this is the feature of group partiality that practically impinges on the success of universal – or cosmopolitan – rights The legal edifice of data subject privacy thus depends on the tolerance of the diversity of the lives it permits for its ultimate success This is, of course, a two-edged sword, since in trying to maintain the freedom of individuals, it is necessary to prevent law-breakers from hiding behind the protection of privacy laws, not merely to prevent those laws from falling into ignominious contempt, but to prevent law-breakers from damaging the lives of others

Liberal toleration, Nagel asserts, makes a demand for the acceptance of an impartiality of a higher order than that which has us recognise the equal value of everyone's life

This higher-order impartiality operates

> precisely on the conflicts between different first order impartialities informed by conflicting conceptions of the good [51]

The problem with presenting this higher-order conception of impartiality is that those who argue for this strong form of toleration tend to place a high value on individual freedom, and limits on state interference based on a higher order of impartiality tends to promote precisely those individual freedoms – like gay rights, abortion, and contraception – which the 'strong tolerators' prefer

This can make some people suspicious that the notion of a higher-order impartiality is a sleight-of-hand to advance what might be seen as politically-correct or radical social values for the sake of having them For Nagel, the heart of the matter is that liberalism

> distinguishes between the values a person can appeal to in conducting his own life and those he can appeal to in justifying the exercise of political power [52]

More generally, and also relevant for our own position, this is the distinction between a system of rules for personal conduct, plus one's *own* conception of the good, and the social projection of those rules as a system of law, in a society of heterogeneous goods the individual level and the social level.

Nagel offers a statement of what liberalism appears to require – that citizens accept a degree of restraint in calling upon the power of the state to enforce some of their profoundly held beliefs against others who do not so hold them, and that the exercise of political power if it is to be legitimate, must be justified on more restricted grounds which can be regarded as held in common

Underlying this, Nagel suggests, is the Kantian Practical Imperative, that one should never treat others as means – and to force someone to serve an end that they cannot be given adequate reason to share is to treat them as a means, even if the end is their own good, as you see it but they do not This underlying requirement is therefore a condition of political legitimacy, and is anti-paternalistic

The interpretation of this which Nagel wants to defend rests upon a classification of grounds for coercion into 4 types

(1) grounds which the victim would acknowledge as valid
(2) grounds which the victim does not acknowledge, but which are nonetheless admissible because the victim is irrational or grossly unreasonable not to acknowledge them
(3) grounds which the victim does not acknowledge, without being irrational, but which are admissible under a higher-order principle which the victim does acknowledge or would be unreasonable to do so

(4) grounds which the victim does not acknowledge – reasonably or otherwise – and which are such that the victim cannot be required to accept a higher-order principle admitting them into political justification even if most others disagree with them

Type 1 coercion is Hobbesian – that is, where each of us is to be forced to do something as part of a practice where everyone is forced to do the same, with results beneficial to all in a way that would not be possible unless it were possible to be assured of widespread compliance Essentially, this is getting people to do what they want to do by compelling them to do it, rather than something they don't actually want to do

Type 2 is "exemplified by the enforcement of criminal law against the wilfully antisocial" and by very basic forms of paternalism In both cases the lack of concern by the recipient of coercion about the harms being prevented is irrational or unreasonable An example would be someone forcibly restrained from committing a crime while suffering from a psychotic episode, who would not be being coerced on grounds which they cannot be given sufficient reason to share, rather, they cannot see the sufficiency

Type 3 coercion is exemplified by public policies based on judgements where reasonable persons can disagree, but where it is also reasonable to allow policy to be determined by a political process in which differing viewpoints are represented and allowed to compete Most of what we think of as political matters – economic policy, law and order – fall into this category; that is, most of our disagreements about the funding and distribution of public goods and their regulation

Type 4 coercion is exemplified by the political enforcement of "religious, sexual, or cultural orthodoxy" Nagel asserts that the liberal case for toleration depends on showing that these grounds for state coercion cannot be subsumed under types 2 or 3, and that consequently, they fail the Kantian test for possible unanimity
That these particular kinds of grounds are not Kantian-unanimous is because they are of that type which are 'aesthetic' or 'metaphysical' in the sense of Hare's fanatic [53], they are *not even in principle universalisable*

If those whom we propose to subject to political coercion cannot be expected to accept the values we wish to further by it, we will be justified only if there is another description of the grounds of coercion that they *can* be required to accept [54]

This cuts to the core of the Golden Rule argument of 'do-as-you-would-be-done-by' and, therefore, to the notion of reciprocity, in the following way The role-reversal question 'How would you like it if someone did that to you' invites the reply 'How would I like it if someone did *what* to me?' Since there can be more than one true description of every action, the selection of the morally operative one is, therefore, crucial

Nagel gives the example that if someone believes that restricting freedom of worship will save innocent people from the risk of eternal damnation that exposure to deviation from the true faith would lead to, then under that description he would, one presumes, want others to do the same for him But under the description of 'restricting freedom of worship', he wouldn't want others to do *that* to him, since it would hinder his path to salvation Consequently, the role-reversal argument needs to be able to be applied in terms which must be accepted by all reasonable (rational) parties as a basis for regulating those disagreements which are not otherwise eliminable.

As Nagel says

I think the problem is that there is no higher-order value of democratic control or pursuit of the good abstractly conceived which is capable of commanding the acceptance by reasonable persons of constraints on the pursuit of their most central aims of self-realization – except for the need to respect this same limit in others [55]

Altruism as a motive does not provide a common standpoint from which to reach the same moral conclusions because it is concerned with the good, and as Rawls has already pointed out, good is heterogeneous (which is why utilitarianism fails) But there is more It has already been observed that utilitarianism confuses impersonality with impartiality, it is not enough to conceive of an ideal moral observer whose individual conception of the good would then be publicly adopted This would be the reduction of liberalism to another sectarian doctrine, which Nagel rejects

The true liberal position, by contrast, is committed to refusing to use the power of the state to impose paternalistically on its citizens a good life individualistically conceived [56]

But Nagel acknowledges that even this is not going to be wholly neutral A state might force people to live according to a particular conception of the good, or prohibit them from living in ways which it condemns Or, it might give preference to the realisation of that conception, by education or other resource allocation, thus involving all citizens and taxpayers at least indirectly in its service Or it might adopt policies for other reasons which have the effect of making one conception easier to be realised than another, leading to a growth in public adherence to that conception as against another, such as the growth of a culture of privacy rights and responsibilities in the UK, different to the rights culture that exists in the USA

The first of these three would tend to involve Type 4 coercion and we should reject it as illegitimate, if the behaviour condemned had no implications for others, and was a matter of essentially private taste The second would tend to be questionable, since it looks too publicly divisive, such as state support for a sectarian religious divide The third might well be unavoidable, and might well be the consequence of adopting the kind of reciprocal liberty we have already discussed, since the effect of constraining political arguments via a mechanism of a higher-order value framework is likely to be ideologically redistributive, or 'politically correct' Those views which would otherwise break the bounds of the framework – like racism, by suggesting that some of the moral 'players' should not be allowed to be counted in – will be placed at a distinct disadvantage It is precisely this conception of a higher-order law which Klug [57] as one of the prime movers behind the HRA 1998 appeals to as the key driver for the future development of the law and politics of human rights and duties Within such a conception of a controlling framework, the DPA 1998 could be said to be in effect 'nested', as the mechanism whereby Article 8 rights are made flesh in the domain of personal information via the European Data Protection Directive (95/46/EC) [58]

Reciprocity requires not just the conferring of rights on others, and therefore the placing of the self under a duty to support the rights of others, but a tolerance of the

lives of others, a forbearance to allow diversity. But the price of toleration-failure could be high The rejection of a rights-and –responsibilities approach to law and the failure of the HRA 1998 legal regime – along Canadian lines, or through the election of a UK government with more draconian intentions – would make the DPA 1998 a very much narrower, rather arid piece of legislation, robbing it of its context and much of its purpose and possibly jeopardising its existence It should be remembered that, while the HRA 1998 might be regarded as supplying a higher-order set of legal values, constitutionally, it is an Act of Parliament like any other, and has no privileged status as an Act *qua* Act It is perfectly capable of being amended or repealed

2.2.2. Rationality

For 'responsible rights' to succeed generally, then, – and the liberty of privacy via the DPA 1998 regime in particular – there needs to be a controlling framework for the formation and maintenance of law which can command support, and which can contain the potential for conflicts between plural values Whatever the temptations towards teleology, this controlling framework has to be rational – a capricious law whose basis was ultimately inexplicable to those who would be bound by it would become an object of contempt The penalties for breaking the law have also to be perceived as reasonable in so far as they are 'appropriate', which is why we ruled out Nagel's Type 4 coercion

The contention of authorities like Klug [59] is that the ECHR-HRA 1998-DPA 1998 regime provides for the reciprocal rights-and-duties approach – 'responsible rights' – which seems to be the desirable means of obtaining the basis for a successful plural society Here, the notion of reasonableness and appropriateness of action finds its expression in the term *proportionality* Generally, proportionality can be understood through the consideration of several criteria applied to cases

(1) Effectiveness – is the measure a suitable means of achieving the legitimate aim? Does it actually achieve its stated aim?
(2) Intrusiveness – is it the least intrusive interference possible?

(3) Deprivation – does the interference deprive the person of the very essence of the right? Or merely curtail one aspect of it?

(4) Balance – does the measure (whatever it is) have a disproportionate effect upon the interests of the affected persons?

Klug [60] puts it thus

> It means – on a strict interpretation of the principle – that any limitations on individual rights must not only be necessary to pursue a legitimate goal but must also not go beyond what is strictly necessary to achieve that purpose

Letting a punishment fit a crime, for example, is an argument it is difficult to refuse, but proportionality requires us to actually mean it. Therefore, we are now being asked to make judgements about value, since it means the appropriate valuation of actions, reactions, punishments Without a notion of *just* valuation, there can be no meaningful justice There is here, though, a further issue Berlin acknowledged the need to try to seek a controlling framework, which we explored via Nagel But to actually make proportional judgements in a legal system is to attempt to make a higher-order scale of value upon which things can be commensurable, if only in the restricted sense of an extensional framework allowing the intensional autonomy of personal values, even when we acknowledge the likelihood of failure to find full political acceptance of this commensurability

Even the conventional English legal notion of reasonableness is a striving for some measure of proportionality, it depends upon what is a culturally acceptable sense of proportion (Hanging for sheep stealing might once have been considered to be a proportional response)

Built into the fabric of the law is the expectation that public authorities will act with reason, and one of the key checks upon this is the existence of judicial review Lord Diplock [61] took the view that the involvement of the court in judicial review was to be restricted to the consideration of decisions which were illegal, irrational, or which had been subject to procedural impropriety The presumption in law is that public authorities must act with reason. Securing this, however, prior to the advent of the test

of proportionality, was greatly complicated for the individual citizen by the severity of the test then applied. This was embodied by the *Wednesbury* [62] principles of judicial review Unreasonableness in the *Wednesbury* sense was defined as

conduct which no sensible authority acting with due appreciation of its responsibilities would have decided to adopt [63]

And as Klug [64] points out, a decision could only be overturned under the principle on substantive grounds, not procedural ones, as indicated by Diplock The burden of proof, therefore, on an individual ranged against a public authority on this basis, to show 'unreasonableness' was very high Diplock's role was to attempt to define irrationality by a public authority as

a decision which is so outrageous in its defiance of logic or accepted moral standards that no sensible person who had applied his mind to the question to be decided could have arrived at it [65]

This still created a steep legal gradient for individuals to climb. Once any procedural impropriety had been addressed, the substantive issues were seldom judged to have been dealt with so outrageously as to justify changes to the law Now, after the introduction of the HRA 1998, the restrictions that can be applied to rights are required to be justified by a legitimate aim and proportional

The concept of proportionality requires that if there are two ways of achieving the legitimate aim and one is less likely to infringe a qualified right, that is the approach that should be used [66]

This will impact on the protection of data subjects in several ways Firstly, as individuals with access to human rights in relation to the actions of public authorities, including courts This will encompass the common law remedies being made available via s2 of the HRA 1998 in dealings between individuals, and between individuals and private organisations Secondly, s3 of the HRA 1998 requires all legislation to be read so as to give effect to the Convention rights, including the DPA 1998. Thirdly, s6 of the HRA 1998 requires public authorities to act in accordance with the Convention rights, which would obviously apply to them in their capacity as data controllers.

The fourth way is directly via the terms of the DPA 1998 itself We have already discussed the Act's origins within the human rights framework, so that its compatibility with the HRA regime is built-in An examination of the Eight Data Protection Principles (Sch1 Part I, DPA 1998) will show the assumption of proportionality, chiefly DP Principle 2:

Personal data shall be obtained only for one or more specified and lawful purposes

DP Principle 3.

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed

And DP Principle 5

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes

Not merely have the rights of access and control under the DPA 1984 and the Access to Files legislation been consolidated, but the discipline of human rights proportionality has been made available But the question of how this would play in a changed political and legal environment should there be a reaction against a rights-based approach in favour of a sovereigntist one, remains For the moment, *Wednesbury* is not entirely lost; but it will only now come into play as a limiting case, where proportionality cannot go

To draw the sting of sovereigntist objections, the HRA 1998 does not permit judges to strike down offending legislation, they may only make a declaration of incompatibility The ultimate responsibility remains with Parliament to propose and amend legislation (Except, of course, in Scotland regarding the Scottish Assembly, and in Northern Ireland regarding that Assembly) Insofar as the origins of the DPA 1998 are human rights friendly, this has no effect – the Act appears compatible The sovereigntist 'longstop' of the incompatibility declaration mechanism is not essentially different to the mechanism at a European level – the European Court

cannot make a member state change the law to accommodate its judgements, but relies on the force of political opprobrium to bring governments into line, and the declaration of incompatibility works in much the same way in a national context

This is the attempt by the British polity to address the issue of balancing the requirement of basic rights with that of political consent to law and government It acknowledges the reality that responsible rights – such as data subject privacy – can only work with and through the consensual mechanisms of parliamentary legislature, and judicial impositions in defiance of parliamentary power would be likely to precipitate a reaction against rights The mechanism is hence a challenge for the oft-quoted British tolerance to prove itself

A further issue of rationality is, broadly, that a law which facilitated criminal acts could not sensibly be described as rational With regard to the privacy of data subjects, criminal acts fall into several categories

(i) Those perpetrated against data subjects by the omissions or commissions of data controllers
(ii) Those perpetrated against data controllers by data subjects
(iii) Those perpetrated against data subjects and data controllers by third parties and others

The thrust of the legislation is primarily concerned with the first of these, in giving effect to the DP Principles The first concern of the Act is the right of privacy of individuals The general savings open to public authorities and organisations through being able to share data without explicit restrictions as to the purpose(s) of gathering and using data or requirement of unambiguous consent have now been curtailed, the presumption of right is in the interest of the private citizen

Actions against criminal behaviour are now to be more closely prescribed by law via the Crime and Disorder Act 1998, including through information-sharing protocols for local authorities and police forces, and through RIPA and the Electronic Communications Act for information-related crime and surveillance The state cannot

act without law, not merely can it not act *ultra vires*, but the *vires* must be proportional, not simply not *Wednesbury* unreasonable.

Determining the boundaries of informational crime means that our view of property and ownership once more becomes important. The NCCL definition of privacy stressed the integrity of the person, which is part of the ECHR Article 5 right of liberty and security of person, but also, if part of that person's personhood is bound up with their control of personal information – such as security of the person – then the ownership, and enforceability of that ownership of personal information – is a key issue Data protection law must in this respect, then, also engage with the ECHR Article 1 of Protocol 1 via the HRA 1998.

If we own the information in our personal (and sensitive personal) data, then we may treat it as our property – to which we are entitled to enjoy peaceful possession, and given the effect of HRA rights on common law, this would probably not just be enforceable against the state (in the form of public authorities) But there would seem to be a difference between unauthorised or unwanted 'trespass' on our 'field' of personal data, compared to our field of crops, for example Some legal opinions (cf Luke Clements [67]) suggest that in the case of real estate the English law of trespass – implying absolute possessory entitlement, and rights of eviction – of travellers, for example, - is not proportional This could be controversial enough in itself, but it is further complicated by the decline of the margin of appreciation available to UK judges In the first case arising out of the HRA 1998 to reach the House of Lords [68], Lord Hope made the following point

> By conceding a margin of appreciation to each national system, the [European] court has recognised that the Convention, as a living system, does not need to be applied uniformly by all states but may vary in its application according to local needs and conditions This technique is not available to the national courts when they are considering Convention issues arising within their own countries But in the hands of the national courts also the Convention should be seen as an expression of fundamental principles rather than as a set of mere rules

It does not follow then that we have to accept the Clements view – our own courts could interpret the Convention rights via the HRA so as to protect the concept of

ownership of property via Article 1 of Protocol 1, but they would then have to do so consistently in other national cases

More importantly for data subjects, however, is that the weakening of possessory entitlement does not seem to hold for personal data – the requirement of consent and mechanisms for redress, including rectification, modification, erasure, and destruction, suggest something much closer to absolute possessory entitlement of and control over personal data and their disposal The distinction is contentious, but the interpretations available under the HRA regarding trespass and under the DPA regarding personal data suggest that this difference exists

The difference between personal and fungible property is ineluctably subjective, such a subjective difference in outlook regarding the ownership of data and its marketing like any other asset distinguishes American and European attitudes to data protection Also, some things which could be conceived of as fungible might actually be regarded as personal – a birth certificate, for example, is personal (and contains personal data) but it is also fungible (replaceable), but the original document might be imbued with a significance that no copy of the original could be. Radin's distinction (and consequently, Munzer's distinction also) needs to be made less fuzzy The distinction is essentially personal –v- impersonal, rather than simply personal –v- fungible Material property can be personal in some contexts and impersonal – and therefore uncomplicatedly fungible – in others A pair of socks is simply replaceable property, even though clothes might be usually thought of as more personal than real estate A thing is fungible because it is impersonal, not the other way round, as a matter of ontological priority

Personal data have this variable character. Some people might not be very bothered if others know they belong to a trade union, others might regard this as being only the business of themselves and a few associates Social contexts are very important in judging when something is to be regarded as sensitive personal data Political affiliations can be a matter of great delicacy – being a supporter of the UDM in an NUM-dominated mining community in the 1980s, for example

This shows the crudeness of the libertarian view of ownership when applied to personal data, and tends to support Ryan's approach; that there is more to personal property than Nozick would have us believe Personal property – and therefore personal data as property – is heavily nuanced by its subjective value and social context

The kind of informational trespass we spoke of just now does, in restricted form, highlight one of the more intractable value conflicts in the realm of privacy There is an obvious tension between privacy and openness, and both can be treated as rights Privacy is protected by ECHR Article 8, and the right of quiet enjoyment of property – which as we have seen, might include personal data – is specifically protected by Article 1 of Protocol 1 But openness is also an important freedom in certain contexts, ECHR Article 10 protects freedom of expression, including the imparting of information, and Article 9 protects, similarly, freedom of thought, conscience and religion These will obtain further recognition in the FoIA 2000, which will begin to come into effect from 2002 onwards.

It is a commonplace – because it is undeniable – that access to information is an important part of a living democracy A certain degree of informational trespass – in the form of journalistic freedom to publish potentially embarrassing facts – is therefore part of the currency of a free society. This is officially recognised with respect to corporate data subjects – organisations – in the form of the Public Interest Disclosure Act But this issue becomes very much more controversial when applied to individuals – UK law now has shifted the burden onto those who would want to reveal information, RIPA and ECA have tightened up the legal framework for state and organisational investigators Sovereigntists might be tempted to argue that legitimate collective interests – national security, community well-being – have been downgraded too far in favour of individualism Libertarians have argued by contrast that RIPA gives government too much power of clandestine interference, and have prophesied deleterious economic consequences for the UK's e-commerce This cuts across party political boundaries, traditional Tories might concur with sovereigntist objections which would support powers of intervention in matters of personal data, whereas free-marketeers tend to emphasise the economically obstructive side of RIPA For left-wing sovereigntists, there might be a suspicion that rich and powerful

individuals might be able to use the new legislation to place much of their affairs – business and personal – beyond legitimate scrutiny

Empirically, it would seem that we are fated to live in interesting times, now that a positive liberty of data subject privacy appears to exist The experience of *Douglas and others v Hello!* [69] suggests that informational trespass towards individuals (not necessarily organisations) will be treated fairly dimly by the courts It has also been reported [70] that a police clerk has been fined £3000 by Llanelli Magistrates' Court for illegally using the Police National Computer to check up on her underage daughter's boyfriend of whom she disapproved

The legislative revolution of HRA-DPA-FoIA-RIPA-ECA attempts to be a rational response to the possible value conflicts and scope for informational crime, before some of the issues arising out of compliance with the law can be examined or conclusions drawn, we need to determine what is at least a working definition of data subject privacy

To underpin a definition of data subject privacy, we need to order our ontological priorities, shaping and determining our intellectual and political commitments Something that is shared with Nozick is a refusal to countenance a lazy Platonism with regard to organisations or societies Kantian persons come before social entities like these, which supervene on individuals as sums-over-histories, and which may then be thought of as emergent This is anti-totalitarian, because it resists the reifying tendency inherent in glib talk about 'society' or 'classes' – or the 'greater good' But in accepting the existence of persons as prior, this also puts property rights in their place, they cannot override the claims of natural persons as ends in themselves, as moral subjects with *dignity*. It is this which forms the basis of Ryan's objection that some things cannot be made objects of a proprietary relationship – we cannot treat others as means and we ourselves cannot be treated as means either We are too involved, the chaos of the lives of those who have sold their stories to the news media – or who live in its spotlight – with stalkers and cranks – shows the dangers of treating personal information as just another commodity Organisations, as dependent on natural persons, have more restricted rights than such natural persons – hence the

refusal to accept Italian-style arguments [71] for legal personality, which might confer full equivalence between legal and natural persons.

Our acceptance of Kantian persons means accepting the importance of the autonomy of action of such persons as rational beings The psychological requirement of privacy is able to be actualised by autonomous action The liberty – inherent in genuine autonomy – of the data subject, and the liberty of the privacy of the data subject, rests upon a fundamental notion of the moral equality of all persons, that they are all equally moral 'players'. But this equality is not itself liberty This liberty entails a freedom to pursue one's own projects, without injury or detriment to others, and the self-improving freedom is a positive liberty There is, however, no positive liberty to impose one person's vision of how life might be lived teleologically on others This is anti-totalitarian also, for it militates against the Nietzschean romanticism of charismatic demagogues who would seek to 'style' whole societies, after the Hitlerian fashion Liberty, overall, would seem to be negative, in a Berlinian sense, if it is to be compatible with autonomy This is given further weight when we consider the need to balance the partiality of individuals with the requirement for the equality of their treatment before the law

Personal space requires a tolerance of the diversity of projects which people might use their personal space for This is why liberal toleration seeks a higher order of impartiality – rules to be held in common for the regulation of public activity are a more restricted set than those which we can use in our own private, personal lives, because our projects are different from those of others We therefore require our law on privacy – and therefore on the control of access to personal data – to safeguard this 'free' space for our personal projects, while at the same time requiring the duty of reciprocity to allow this freedom for others

We began with the NCCL definition of privacy; it might reasonably be asked how this could be extended or ramified to provide for the kind of definition that is being sought

Solitude would seem to be not merely the right to have one's physical senses unmolested in any private place (which is linked to the Article 1 of Protocol 1 ECHR

right of quiet enjoyment) but also to freedom of thought and reflection, free from social pressure and coercion of others One is tempted to say that with the forbearance and reciprocity we have already spoken of, one should not have one's senses *molested* in a public place either

Intimacy would be reflected in the ECHR right of family life and in the UN Declaration of Human Rights It would be necessary for the maintenance of emotional health

Anonymity is closely linked with the requirement of autonomy – the freedom of action of private persons in matters that concern themselves, privacy is not cashable without autonomy It is interesting that acquiring freedom of action is the significant feature of the teenage years, and the mature use of that freedom the mark of adulthood

Reserve would also seem to need to include freedom from psychological pressure and from physiological interference – both matters of concern for the UDHR and the ECHR regarding the prohibition of torture, and therefore freedom from Nagel's Type 4 coercion Freedom from psychological pressure could mean freedom from undue commercial advertising influence, as with Sweden's strict laws regarding advertising to children It could also be possible grounds for justifying stronger measures to enforce anti-direct marketing measures Furthermore, it could also mean freedom from scrutiny, and is therefore linked to solitude and autonomy

It is striking that these four aspects of privacy are all concerned with the *dignity* of a person, which was Munzer's point, and one which Klug has made [72] Dignity takes us beyond the libertarian conception of the commercial and the rule of market forces, which is the Kantian core of the argument in Ryan, and Munzer, what the whole matter of privacy is about and what it is for

Privacy of personal information is a general requirement for confidentiality – which links directly to a general principle in the common law in tort, but also to the DPA itself It is a means by which the previous aspects of privacy can be realised

Missing from the NCCL list is an explicit commitment to *reciprocity*, an up-front respect for the privacy of others would be a 'responsible rights' approach This reciprocity involves value-tolerance for others' private lives and religious beliefs and means forbearance in practice Reciprocity also means that certain privacy rights must be qualified in public places, including workplaces – our behaviour is likely to be different in different social contexts, as a matter of different degrees of *intimacy* Only by this fitting of behaviour to social context can we expect to give the rights of others their proper weight – and therefore give due respect to others' sensitivities and solitude – their personal space Necessarily this entails no taking of unfair advantage, and therefore precludes any criminal abuse of privacy rights

Public interest defences to release of personal information and hence to breaches of privacy could only be justified if there were good grounds for suspecting unlawful behaviour, acts or conduct or specific hypocrisies – mere media prurience would not be sufficient The adultery of a government minister would only be a legitimate target were the minister a supporter of puritanical moral standards for others, for example

Connected to this reciprocity would be an explicit commitment to *proportionality* since recognition of the need and occasion for reciprocity requires a sense of when and how much, which entails a sense of moral proportion, of judgement.

CHAPTER 3: COMPLIANCE

In gauging the effectiveness of the legal measures introduced to protect the privacy of data subjects, the extent to which compliance is likely to be forthcoming is related directly to the legitimacy of the means and the end to which the law is directed The ground on which the legitimacy of these measures is fought out is between privacy and openness, and it is on this territory that the efficacy of the legislation will be tested and where ultimately the view of data subject privacy outlined at the end of the previous section will be exercised

3.1. Avoidance and resistance.

Some avoidance of, and resistance towards, the notion of privacy is sanctioned by law. The principal ground on which this is now considered to rest arises out of Article 10 ECHR (Article 10(1))

> Everyone has the right to freedom of expression This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers

Importantly, however, this is a qualified right (Article 10(2))

> The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence

The list of restrictions that are 'necessary in a democratic society' specifically refers to the rights of others – private individuals – but also to the rights of organisations under the general principle of confidentiality Also, it directly engages with the concept of duty and responsibility, these are not merely suggested but are named Part of this duty is to respect the right of privacy in Article 8 ECHR

This balancing is apparent in the DPA 1998 itself [1] S32 of the Act is the vehicle by which public interest issues – in the form of journalism, literature and art – can be realised, since the consent of possibly criminal data subjects to the investigation of their affairs is unlikely to be forthcoming The DPA therefore disapplies the

conditions for the processing of sensitive personal data in Sch2 of the Act from the media Consequently, it is not necessary (as already stated) to obtain the consent to processing of the data subject, but also the media can bypass the requirement for the processing to be necessary to protect the vital interests of the data subject This has led to the publishing of details of peoples' lives making it possible to harass them in their own homes – such as paedophiles – driving them 'underground' and nullifying the effect of the sex offenders' register Media self-righteousness about the 'public interest' here has actually damaged the real public interest of the police and other stakeholders knowing the whereabouts of such people and being able to exercise meaningful control

The exemption also means that the following provisions of the Act will not apply

(a) the data protection principles, *except* DP principle 7 concerning the security of the data concerned, since only those covered by the exemption can benefit from it, and unauthorised persons would fall within the full scope of the provisions of the Act
(b) The subject access provisions in s7, since avoidance of the data subject's access rights is the purpose of the exemption This leads naturally to
(c) The exemption from s10, the right to prevent processing likely to cause damage or distress, the embarrassment of caught-out politicians (like Jonathan Aitken, Jeffrey Archer, or Peter Mandelson) could not be avoided given the nature of what was revealed
(d) S12, rights in relation to automated decision-taking, though the role of this in relation to journalism, literature or art is less easy to understand
(e) Transitional rights in s12A (created by Sch13); interestingly, this means that media data controllers are exempted from having to correct or destroy manual data exempt under the transitional period arrangements This is a matter of concern, while journalists might be thought of as wanting the information they have to be as accurate as possible – to avoid libel – the story of sexual assault relating to the former MP Neil Hamilton, and his wife Christine, demonstrates how badly this can fail. The juiciness of the idea prevailed in the first instance over caution about its veracity. More worrying was the way in which the story appeared to leak from the police to the press – the avoidance of privacy had

crossed from being legally sanctioned into a grey area of public interest bordering on illegal resistance to the protection of the rights of the data subjects There seemed to be almost a presumption of guilt.

(f) S14(1)-(3) right of rectification, blocking, erasure or destruction In the Hamilton case above, this was not a problem in the matter of the journalism itself, one expects journalists to pursue interesting material The problem, potentially, was with the means by which the story came out The Hamiltons were criticised for themselves conducting a defence via the media, but it is difficult to see what else they could have done, given the nature of the allegations, and the *schadenfreude* of some of the press.

Obviously, to benefit from the exemption, personal data processed for the 'special purposes' in s3 of the DPA 1998 – journalism, artistic or literary purposes – must satisfy the following 3 prerequisites

(a) the processing must be undertaken with a view to the publication by any person of any journalistic, literary or artistic material
(b) the data controller must reasonably believe that, having regard in particular to the special importance of the public interest in freedom of expression, publication would be in the public interest, and
(c) the data controller must reasonably believe that, in all the circumstances, compliance with the provision in question is incompatible with the special purposes

Carey [2] continues that s32(4) would seem to prevent "so-called gagging orders" within 24 hours prior to publication by providing that proceedings against a data controller under any of the provisions to which exemption relates will be stayed if the relevant personal data are being processed·

(a) only for the special purposes, and
(b) with a view to the publication of special purposes material which had not, excluding the 24-hour period prior to the proceedings, previously been published by the data controller

The proceedings will remain stayed until either the Information Commissioner makes a determination (under s45) that the personal data are not being processed in compliance with (a) and (b) above or the data controller withdraws their claim to have complied with (a) and (b) above

There is a further legal route of avoidance which brings us closer to the broader framework of freedom of information and the FoIA 2000, but remains linked to journalism and the public interest. This relates to historical and other research, and in the preparation of statistics. Persons pursuing lines of enquiry are able to evade some of the provisions of the DPA 1998 via s33, relating to personal data processed "only for research purposes" These research purposes are not defined in the Act, but s33(1) states that they include statistical or historical purposes

Carey [3] states that

A disclosure of personal data to any person for research purposes does not prevent the exemptions from applying, nor does a disclosure to a data subject or a person acting on his behalf

Research is exempted from the second data protection principle that is, simply, that data must not be processed in a manner which is incompatible with the purpose for which it was obtained S33(2) provides that the processing of personal data for research purposes will not breach the second principle if the processing complies with certain 'relevant conditions' as set out in s33(1) These are defined *negatively*·

- that the data are not processed to support measures or decisions with respect to particular individuals
- that the data are not processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject.

Research is also exempted from the fifth data protection principle personal data processed for research purposes can be kept indefinitely Also, s33(4) specifies an exemption from the subject access provisions in s7 Furthermore, there is a continuing exemption after the end of the First Transitional Period (23 October 2001) for historical research, providing that the 'relevant conditions' are met Birkinshaw [4]

points out that research on these terms must be made available such that the results do not identify individuals, who must remain anonymous

The FoIA 2000, in s62, provides a definition of 'historical record'

a historical record is a record which is 30 years old counting from the calendar year following that in which it was created Where records are kept in a file, the 30 years are reckoned from the calendar year following that in which the most recent was created

The interlocking nature of DPA and FoIA is evidenced by the fact that in the FoIA, s40 points applicants for personal information towards the DPA – the data protection regime for personal information is nested within the freedom of information framework S40 creates an *absolute* exemption in the case of data within paragraphs (a)-(d) in the definition of data within s1(1) DPA 1998 and disclosure to a member of the public would contravene any of the data protection principles There is also an absolute exemption in the case of data added by the FoIA where the disclosure would contravene any of the data protection principles but for the exemption in s33A DPA 1998 (added by the effect of s70 FoIA 2000), this only applies to manual data introduced into the scope of data protection by FoIA and which is held by public authorities

Birkinshaw [5] points out that where a request is for personal data *not* covered by DPA or FoIA it is *not* exempt – but it is difficult to think how this would apply, given the scope of the DPA. Where the request *is* for data covered by the DPA and FoIA, but the data *is* exempt from s7(1c) DPA by virtue of *any* provision in Part IV of the DPA, it *is* exempt from disclosure under FoIA, but the exemption is not absolute – it is subject to the public interest test

A further point regarding the balance between privacy and public interest is that for s34 DPA, s72 FoIA inserts, after the word 'enactment', the rider that this is other than an enactment contained in the FoIA itself, ensuring that the law is not circular, and the privacy regime of the DPA is not vitiated FoIA has little to say in itself about personal data – its primary function is to make impersonal information more widely

available What it does do, by having the personal data regime placed within it, is to create a framework which encompasses the continuum of information

Public interest can impinge upon the privacy of the data subject via the provisions for journalism within the DPA 1998 The concern is that, while the framework appears a rational response to the issue of balancing privacy and public interest, a broader rationality in the media is patchy at best Public interest, however, has two sides Investigating the hypocrisies of politicians and the scions of industry – or just giving us the human interest of a good biography – to inform us, has a corollary in investigating the public for our protection. We admit the principle of policing our privacy for our safety This ranges from store detectives observing our behaviour, through CCTV, police information-gathering, to national security, vetting and anti-terrorist measures

Exemptions for national security are, not at all surprisingly, very far-reaching It is exempted from

The data protection principles
Part II (the rights of the data subject)
Part III (notification)
Part V (enforcement, s28(11) quite clearly rules out any application of PartV)

More radically, s28(1) clearly shuts off the effects of s55 concerning criminal offences of unlawfully obtaining personal data (and see s55(8)). Notwithstanding the requirements of RIPA 2000 regarding the regularising of intercept powers and so on, this is – as Birkinshaw emphasises [6] – an exclusion from the DPA where all the exemptions apply Furthermore, a certificate signed by a minister of the Crown stating that the exemption was required for national security shall be regarded as conclusive evidence of that fact of the exemptions applying. The person affected by the certificate may appeal to the Information Tribunal, which will apply the principles applied by a court on an application for judicial review. The certificate must be related to the statutory purpose; it must not show bad faith, an abuse of process, or ulterior intent Conceivably, with the arrival of the HRA 1998, it must not show

disproportionality by the executive The problem, as Birkinshaw avers, is that the facts are effectively under the control of the executive

Closer to most of the public than national security is the day-to-day reality of law and order The informational aspects of this reality are controlled by the Crime and Disorder Act (CDA) 1998 Local authorities are charged with a statutory duty to do all that they reasonably can to prevent crime and disorder in their areas (s17 CDA 1998) The Act also requires the establishment – with the police and other stakeholders – of local crime and disorder partnerships to formulate and implement crime and disorder reduction strategies (s6 and s7), anti-social behaviour orders (s2), and local child curfew schemes (s15 and s16), which are themselves subject to new guidance (autumn 2001) from the Home Office S3 and 4 cover sex offender orders

In order to meet the objectives of the CDA 1998, many public authorities have entered into information-sharing arrangements The power to do this is contained in s115 CDA 1998, which states that·

> Any person who apart from this section would not have power to disclose information
>
> (a) to a relevant authority, or
>
> (b) to a person acting on behalf of such an authority
>
> shall have the power to do where the disclosure is necessary or expedient for the purposes of any provision of this Act

'Relevant authority' is defined in the Act as a chief officer of police (or the Scottish counterpart), a police authority, a local authority, a probation committee, a health authority, or person acting on their behalf, so long as such a disclosure is necessary or expedient for the purposes of any provision of the Act

This section of the Act does not, in terms of the power to disclose, enable any of these authorities to *demand* information from a third party, nor does it *require* any of the authorities to share information What it does do is to provide these public authorities with the *vires* to share information; this has the effect of satisfying at least one element of the lawfulness requirement of the first data protection principle But s115 does not override the existing legal safeguards that apply to *personal* information, which is still protected by data protection legislation, laws of confidence and

defamation, and so on Interestingly, the Home Office guidance [7] at point 5 9 states that the disclosure of information

need not be restricted to cases where the end result is a prosecution under criminal law

The example given at 5 10 is that of eviction proceedings under the Housing Act 1985 (as amended by the Housing Act 1996) on the grounds of breach of the tenancy agreement involving criminal behaviour, since this would come within the scope of the prevention of crime within a local authority's area, the disclosure powers would apply

Interpreting the interactions of the CDA and the DPA, and the common law duty of confidence, is an area of considerable concern for public authorities – central government has effectively decentralised the task of interpretation and balancing of rights and interests to local government level

The Home Office guidance at 5 17 states that the crime prevention exemptions of the DPA 1998 mean that the non-disclosure provisions of the DPA do not apply. But in 5 18 any request for personal information whose purpose is the prevention or detection of crime should specify as clearly as possible how failure to disclose would prejudice the objective In the case of the local authority eviction, if the local authority housing department wanted information from the police, the request should make it clear why the information was necessary for the proceedings (they might fail without it) and why a successful action would prevent crime (the removal of the offender from the estate, for example) Only an overriding issue, like preventing crime, and preventing threats to third parties, could justify the overriding of the requirement to seek the permission of the data subject (in this case, the offender) with regard to the disclosure of the personal information about them

S17 of the CDA 1998 creates the duty to do all that is reasonable to prevent crime and disorder in its area on a local authority, and this is a legal duty for which compliance is required, in terms of Sch3 of the DPA 1998 for the processing of *sensitive* personal data, as well as the legal obligation in Sch2. But this can only be *activated*, as it were, for a *specific instance* – it cannot be used to justify a *general* sharing of personal, or

sensitive personal, data Data shared have to be for a particular purpose, and relevant to the point of that purpose, to satisfy the requirement of the third data protection principle – and this relevancy and adequacy is itself a manifestation of proportionality

Both the Home Office and OIC guidance set out checklists for setting up information-sharing arrangements, and a key process to be addressed in both is how the mechanism is to be engaged The OIC guidance requires not merely that appropriate security measures need to be taken – in line with the DPA requirements – but also that information disclosed for the purpose of the anti-crime initiative does not become the general property of each of the relevant authorities and that other staff of the authorities who are not part of the initiative should not have access to the information.

So far, we have considered legal exemptions from the data protection regime – legitimate forms of avoidance – and we have not yet addressed the legal regime of RIPA 2000, which will be examined later But we must consider the subversion of the controls and restrictions placed on personal data The Information Commissioner's Office is well aware of the potential problem, particularly from private data matching of information otherwise publicly available Davies and Oppenheim [8], in their report to the then Office of the Data Protection Registrar, investigate the possible misuse of publicly available registers in some detail

Perhaps the leading source of concern in this regard, because it affects the vast majority of adults, is the Electoral Register It is widely available for public inspection and can be found at local and central reference libraries, Citizen's Advice Bureaux, local authority offices and Crown Post Offices Alive to the possibilities for stalking and harassment, the Greater London Authority's new partnership register will enable personal information to be kept confidentially

Davies and Oppenheim [9] point out that one Elections Officer did not think that providing the Electoral Register in electronic form to companies wishing to purchase it was ethical, since their use of the data was not what Parliament had intended – hinting at a possible conflict between commercial use and electoral purpose under the second data protection principle Worse are the inferences that companies or

individuals may try to draw from the information, one thinks of 'postcode lottery' effects for insurance purposes, where people fall within an area identified with car crime, for example Cross-referenced with telephone directories, this is quite a dataset for salesmen and women to get their teeth into This issue, of the electoral register being available to companies, has now been the subject of a court ruling [10] A retired accountant in Yorkshire removed his name from the electoral register because he did not want to receive junk mail, as his local authority refused to promise that it would not sell his name and address to credit reference agencies and direct marketing companies The local authority was found to be in breach of the man's right to privacy under Article 8 HRA 1998, but also that it resulted in a disproportionate and unjustified restriction on his right to vote Significantly, the judge found that local authorities have been selling registers without following EU rules on the subject, which the Government had failed to enact fully in the DPA 1998 The DTLR (now ODPM) announced that they were studying the ruling very carefully

One problem identified by Davies and Oppenheim [11] has now been addressed Some people wished to be able to use a postal vote to avoid having to go to a polling station so that they did not have to meet estranged spouses or partners, with the risk of verbal, or indeed, physical abuse Prior to the 2001 General Election this would have required them either to be away from home, or to risk perjury by saying that they were but not actually being so From the 2001 General Election – and local authority elections - this has now been changed [12] Omissions from the register – such as Polish settlers during the 1930s, who were never naturalised – can lead to problems with obtaining credit, sub-addresses which have not been correctly identified by credit reference agencies can also cause problems

The Companies Act 1985 requires the maintenance of a Register of Directors & Secretaries (s288 to s290) Access to the Register must be provided at the company's *registered* office; while access for any member of the company is free, non-members are required to pay a fee [13] Personal data shown for Directors and Secretaries of companies include the usual residential address and, for Directors, details of other directorships held by them Private cross-referencing with electoral registers, telephone directories, possible 'Who's Who' entries, and other commercial directories available in libraries, can enable quite a comprehensive picture to be built up The

Register of Bankruptcy Orders offers similar potential This can be inspected at the local Official Receiver's Office, a search request may be made in person at the local office or by post or fax to the Birmingham-based Insolvency Service An individual making such a request would be required to provide their full name and address, and the name(s) and address(es) of the bankrupt, and if known, the date of birth, age, occupation, and trading details of the same To rule out individuals of the same name, the Insolvency Office suggests that as much information as can possibly be given about the bankrupt should be. Searches can only be conducted using a personal name, and the information is computerised Significantly for control of access, the search is conducted by a member of staff for the requestor, who is given a printout of the search if it is successful Davies and Oppenheim found that a request for information about a large number of individuals (say 10) would be met with

> a marked reluctance by the Office to do such a search [14]

However, asking the requestor to provide a legitimate reason for the request left the issue of how such a reason would be established unclear The Register is not sold to any companies The arrival of the DPA 1998 has led to the introduction of a 5-year time limit on public inspection from the date of the relevant bankruptcy order; this would appear to address the issue of proportionality inherent in the fifth data protection principle, on data being kept for no longer than is necessary

The activities of animal rights activists against company directors in the case of Huntingdon Life Sciences has led the Government to introduce a clause in the Criminal Justice and Police Bill [15] to keep their home addresses private if they are at genuine risk of violence, the home address would only be available to organisations like the police

Greater disquiet – raising the legitimacy issue once again – has been expressed regarding the effects of RIPA 2000. Amongst other measures, this almost totally replaces the Interception of Communications Act 1985 [16]. RIPA makes unauthorised interception a criminal offence, interception without lawful authority is made a tort under s1(3) Relevant to many organisations with intranet facilities, under s1(6), the controllers of private communications services are excluded from criminal

liability where they make an unauthorised intercept but their action will remain tortious unless they put parties on notice that their calls are likely to be monitored Regulations [17] have been issued by the Secretary of State under s4(2) authorising the interception of telecommunications in very wide terms for the purpose of monitoring business calls Authority can be given by the consent of the person who made or received the communication, where there are reasonable grounds for believing that consent has been given, or by warrant of the Secretary of State

A safeguard for the principle of privacy is that unauthorised disclosure of information obtained through intercepts is a criminal offence under s19 RIPA – except that, as Birkinshaw intimates [18], how is one to obtain evidence to prove unlawfulness when those committing the breach are likely to be in the intelligence services or closely connected police elements like Special Branch?

RIPA has been seen as one of the most controversial of the Government's information measures The power to demand that encrypted material be rendered intelligible or that a decryption key be handed over has occasioned condemnation in the computer press [19] Furthermore, non-disclosure when requested and tipping off another person about a notice requiring disclosure where secrecy is required are offences However, the objection to what the Government has done appears not to be based on a concern for data subject privacy, but on the interference it represents in the operation of seamless global e-commerce This attitude should make us suspicious that the cyberlibertarianism we tend to hear about in relation to the internet and electronic communications generally, is nothing but special pleading by an e-commercial elite

Brown [20] refers to the rise of an 'overlay culture' which originates from American commercial libertarianism, the idea that the freedom of the internet is some unstoppable tide of a new democracy is nothing of the sort, and has instead allowed the e-commercial elite to bypass conventional democratic forms and controls His predictions of a virtual *kulturkampf* now look prophetic

> Many digerati look ahead to a global village but ignore the chaotic splintering of identities, the clash of expectations, the deepening resentments and broken dreams that surround them on all sides The seeds of their global monoculture are being planted in a soil that lacks the essential nutrient of social

consensus that they will need in order to grow This consensus will be elusive if not impossible to reach [21]

That this rejection of conventional legal forms has probably encouraged the kind of terrorism witnessed on 11 September 2001 has given the lie to the hubris of the new electronic frontier

Brown, in naming some of the self-professed 'anarcho-capitalists' [22], shows that what they seem to be offering is a globalised social-Darwinism The legitimacy of their views might now be open to question in a way that would not have been possible before the events of September 2001 The e-commerce elite were scarcely friends of data subject privacy where this acted as a brake on marketing and the information-gathering required for its sophisticated modern deployment Brown goes on to quote MIT's Nicholas Negroponte [23] that we will each become an audience and a market of one This vision of stultifyingly commercialised moral solipsism is simply so charmless and empty of human warmth and life as to be risible, save that it is offered so portentously The triviality of this vision – compared to the texture of real life – has been put into a proper perspective by the sheer force of events. Essentially, the new political and economic realities make the notion of greater electronic regulation look less draconian and much more in tune with public opinion, certainly in the UK The threat which was held up by the politicians as the object of their measures has turned out to be shockingly real

As Jack Straw – when Home Secretary – put it, when replying to criticism in the computer press [24]

Simply put, RIPA aims to balance individual rights, the interests of business and those of law enforcement, to ensure that UK cyberspace provides the safest environment for e-business

Straw continued RIPA does not mean that all ISPs would be required to monitor all e-mail traffic, and there would not be some special centre created to access all e-mail Rather, some ISPs might be required to maintain an intercept capability, and only after consultation with individual providers on the precise terms of the requirement

RIPA does not permit 'unfettered' electronic surveillance by the security services, as Straw said [25]

> Interception warrants require my personal authority and may only be authorised if they meet one of the narrow criteria set out in the Act – a threat to national security, a threat to the nation's economic well-being, or to prevent or detect serious crime

This would hold as an argument provided that the criteria were sufficiently defined to narrow them, but the general point remains interference with private electronic transactions might be necessary in a democratic society – as recognised in Article 8 ECHR Sober reality has made the more *outré* pronouncements of the cyberlibertarians sound histrionically shrill Threats of the kind Straw refers to could destroy the foundations of the liberal framework upon which the values and practices of the human rights approach to law depends, which itself seeks to preserve the privacy of data subjects Arguably, the sort of measures set out in RIPA fall within the coercion types 2 and 3, examined in Chapter 2, rather than Type 4.

The threat to meaningful privacy seems largely to come from the attitudes of business, or other, self-appointed individuals, like activists or terrorists, rather than chiefly from the actions of democratically-elected governments Gauthronet and Nathan, in the ARETE study [26] have indicated the widespread use of *cookies* files by companies to enable them to collect information which then makes possible very detailed profiling of customers' preferences and interests When, however, ISPs like AOL (cited in the ARETE study) attempt to show social responsibility, and carry out their legal obligations, they receive a great deal of criticism from cyberlibertarians for doing so If the internet cannot police itself against terrorism or paedophilia (to take the most glaring examples) then someone must.

There is an argument in favour of basic traceability on the internet – the notion of anonymity would ultimately create the distinct likelihood of

> uncontrolled deviancy, accusations, denunciations and defamation [27]

Such a capacity to evade personal responsibility via such a pernicious form of anonymity could scarcely be a way of securing rights. This solipsistic misuse of privacy is the most disturbing form of resistance to compliance with information privacy legislation

3.2. Compliance and enforcement.

So far, we have spoken about what privacy for data subjects might mean and how the balance between privacy and publicity might be managed within the law We have also looked at the concerns arising at the boundaries of the law, where privacy and publicity shade into illegality The question we can now ask is what is the reality of compliance for the public authorities which are the primary subjects and objects of the HRA-FoIA-DPA regime? More specifically, how does this affect those public authorities we experience most of the time, namely, local authorities?

The double-edged quality of public interest is very apparent here, the public expects local authorities to safeguard privacy while preventing fraud and other crime, and to do so in a manner which is free from unnecessary 'bureaucracy' in the colloquial sense Privacy might have a price in additional administration which conflicts with the desire for less regulation, and also for the prevention of crime The balance between these is seemingly always having to be re-struck; their reconciliation is not simply an academic exercise, but a real-world resolution of a Berlinian value-conflict

A principal means of protecting privacy consists in the restrictions on data sharing, to restrain data matching. The Office of the Information Commissioner has issued a battery of guidance about information sharing and the possible secondary use of data The question of the secondary use of the electoral register has already been considered, and the matter is subject to a legal judgement which could lead to considerable restriction on the use of this information The other significant purpose for which personal data is likely to be collected on a wide range of adults is for the administration of *council tax* The principal powers under which local authorities operate this derive from the Local Government Finance Act 1992, but the OIC acknowledged that, given the volume of questions surrounding the use of council tax data, specific guidance from a data protection viewpoint was required [28]

This reiterates that local authorities must, as entities created by statute,

> have specific statutory authority to use or disclose information acquired by virtue of their powers to charge and administer Council Taxes for any purpose

In short, local authorities must not act *ultra vires* with respect to the council tax The local authority may, however, in its capacity as a *billing* authority, make use of other information in its possession (except that held by it in its capacity as a police authority), for council tax purposes Any information so obtained may only be used or disclosed for council tax purposes, unless any specific statutory authority exists allowing secondary disclosures or purposes No power exists within the LGFA or the Regulations to make disclosures of personal data for other purposes, which are held for council tax purposes Para 17, sch2 LGFA allows for regulations to be made for the supply of relevant information to any person who requests it for another purpose, but personal data are specifically excluded

Ibrahim Hasan, the Principal Assistant Solicitor at Calderdale Council, has made reference to s111 of the Local Government Act 1972 [29] which allows a local authority to do anything which is calculated to facilitate, or is conducive to or incidental to, the discharge of any of its functions Function

> embraces all the duties and powers of a local authority the sum total of the activities that Parliament has entrusted to it [30]

Hasan has sought legal opinion from Andrew Arden QC with regard to the restrictive interpretation which the OIC has placed on the use of council tax data. The latest advice from the OIC, however, quite specifically closes off this approach

> this Section [s111 LGA 1972] does not allow the exercise of powers derived from one statute for another statutory function In particular it would not allow personal data held for Council Tax purposes to be used as a resource for other local authority purposes, even given the consent of the Council Tax payer [31]

Clearly, the Commissioner takes the view that use of the council tax personal data for any purpose other than the council tax (except where specific exemptions apply

regarding fraud and crime) is contrary to DP Principle 2, and therefore any such use would be *ultra vires*, and hence also a breach of lawful processing in DP Principle 1

The OIC guidance concludes

> The Commissioner recognises the restrictive nature of the advice which she has received and of the difficulties which this may cause Councils The Commissioner also recognises that the effect of this advice may run counter to the encouragement given to public bodies in the Modernising Government White Paper to share and make more effective use of information which they hold The Commissioner would therefore advise local authorities to make their representations for a change in the law to the government through the usual channels [32]

The Commissioner's dusty salvo suggests that 'joined-up' government is some way off yet, frustrating local government's ability to deliver the 'low bureaucracy' seamless services that the public claim they want The OIC advice also stymies a low-tech data sharing between departments, a local authority could not use its council tax database to help it trace its own debtors unless these were council tax debtors, for example The Representation of the People Act 2000 does, however, via its Regulations, allow electoral registration officers to use council tax records for the purposes of registration duties, curious how some legislation can permit information for one statutory function to be used for another, but other legislation cannot

Circular 611 from the Local Government Association has asked local authorities to give examples of how legislation is hindering e-government, with the intention of seeking to persuade the Government to change the law

Council tax data may, of course, be disclosed for the purposes of the prevention and detection of crime, and by the apprehension or prosecution of offenders (but not the cheating of local authorities, and other payers, by not paying bills apparently) to the extent that s29 DPA 1998 applies This engages with the s115 CDA 1998 issues raised in the previous section 2 1 The Home Office guidance [33] at point 5 23 sets out a checklist of issues which should be addressed when information sharing arrangements are drawn up Disclosure of personal information must be registered with the OIC – and the new notification system permits the listing of partners with whom data might be legitimately shared. Compliance with the crime and disorder

purposes of the CDA 1998 is a 'legitimate basis' for disclosing personal and sensitive personal data providing that it meets the other requirements as to purpose, namely that it is

- adequate, relevant and not excessive
- necessary (where depersonalised information would not achieve the purpose)
- used only for the specified purpose

The Leicester City Council Community Safety database – as an example of good practice [34] – holds 'core' data on victims, offenders and offences, provided by the community safety 'partners', who can obtain access to the database once they have signed up to the Code of Practice which sets out the rules for access The partners comprise the police, probation service, social services, the Magistrates' Court, and the City Council

The preferred structure would seem to be that of a protocol governing the general framework of the information sharing initiative and a Code of Practice to provide the day-to-day rules of access and operation The Code must be robust enough to answer the detailed question at 5 23 (viii) of the Home Office guidance checklist concerning how compliance with the other data protection principles not so far engaged in 5 23 (i-vii)

The key safeguard over the release of personal data – and upon which the legitimacy of data protection law rests – is that it is done with our consent, and where consent is overridden to secure other desirable ends, that the conditions and controls for this are reasonable The requirements for ensuring consent and confidentiality can have some far-reaching effects on the practical handling of data. These effects can be largely explored under the 'heading' of *third-party* effects

The phenomenon can manifest itself in circumstances where a data subject makes an access request for information which contains references which could identify another individual If this 'third party' individual has no objection to being identified, no problem really arises Mostly, though, the third party here would have no reason for

being identified – such as the details of a social housing mutual exchange, where details of the family of the third party would not need to be transferred ordinarily to the data subject making a request for access to their tenancy details (since those details would belong to another tenant).

More complex – with potentially more risks – would be a request from a tenant for access to tenancy details, where there were details of an estranged partner and a forwarding address the tenant making the subject access request did not have In the first instance here, the data controller would – in accordance with the DPA and the OIC guidance on third party information [35] – consider to what extent it would be possible to give information without compromising the third party Neighbour complaints, or information given to social services, would be a case in point, since even giving out a 'depersonalised' version of a complaint might be sufficient for the data subject to identify the complainant.

This is a manifestation of what could be termed the *'tipping-off'* problem A more pernicious example would be where the data controller – in seeking the consent of a third party to a release of information – precipitated the third party to take some illegal action against the data subject making the access request The mere act of being asked could trigger off an act of violence against the data subject, and the data controller might have had no reason to exercise a particular prior caution (rather than a general one) in seeking the third party's consent, since there might have been no evidence available to the data controller to suggest that such a problem might exist A further instance arises with enquiries – including subject access requests – made by a person on behalf of the data subject The third party might be prepared to consent to the disclosure being made to the data subject, but not to the proxy One solution to this case of the question of consent is to disclose directly back to the data subject

One of the practical considerations in such cases concerns discussing rent accounts with tenants of local authorities – these would not be discussed with a proxy unless there were some written authority, like a declaration of power of attorney, or a signed transcription of a verbal understanding

Mrs X, a joint tenant of a council house, contacted her MP with regard to a rent issue that had arisen with respect to the tenancy The MP telephoned to the local authority and was told by a rent officer that, since the council had been given no consenting authority from the tenant to discuss her rent account with anyone else, the matter could not be discussed with the MP until this was forthcoming This was confirmed to the MP by the rent officer's manager, who pointed out that if the council were to be prosecuted for illegally divulging information, it would be the council officers who would be fined, not the MP. This position was expressed in reply to a query from the MP by the chief executive of the authority

This looks *prima facie* rather 'jobsworth', but a case quoted in the data protection press [36] reveal the lengths some people will go to in the illegal pursuit of information

A policeman called with information about an alleged assault on a student and asked for the student's home address The policeman gave the telephone number of his police station in Devon, so that his identity could be verified On calling back, a person with a Devon accent referred the return call to the personnel office, who verified the identity of the policeman The student's address was then disclosed It turned out, after the student had complained about harassing telephone calls, that the telephone number of the police station was a callbox and all the parts were played by the initial caller, including sound effects for the transfer of calls on a switchboard

The other chief form of third party effect would be where a professional opinion had been given about a data subject, such as a medical report, or an employment reference These tend to receive special treatment under the law by way of exemption, and show an important connection between consent and confidentiality. The OIC guidance [37] states.

Where consent has not been given and the data controller is not satisfied that it would be reasonable in all the circumstances to disclose third party information without it, the safer course for the data controller is to withhold the information

The guidance acknowledges that this could lead to scrutiny by the Commissioner, and possibly to enforcement action Should the Commissioner decide that disclosure should not be made without consent, and the data controller continues to withhold the information, the Commissioner's view

Where the Commissioner serves an enforcement notice requiring the data controller to disclose, such a disclosure should be protected by a defence of compulsion of law against an action brought by an individual for a breach of confidentiality.

One area of practical concern regarding third parties and consent for local authorities and utilities has been change-of-address The emergence of the Electronic Government Initiative from UK central government has brought this to the fore, and the latest position would appear to be that organisations like ihavemoved com, which rely on a broad group of signatories, including utilities and local authorities, are now legal provided that they satisfy the OIC Indeed, the Government will find it practically impossible to meet its e-government targets without them
Currently, the safest way of preventing local authority tenants from avoiding paying for their utilities – and letting the council continue to pick up the bill from when the property was void – is to notify the utility when the void period ceased, so that the utility can then bill 'The Occupier' This way, no possibility of transfer of personal data breaking the bounds of consent occurs.

The only condition which would really justify bypassing consent – where crime or fraud were not at issue – would be to protect the 'vital interests' of the data subject or another person This concept can only be invoked where

- consent cannot be given by, or on behalf of, the data subject
- the data controller cannot reasonably be expected to obtain the consent of the data subject, or
- in a case concerning the protection of the vital interests of another person, consent by or on behalf of the data subject has been unreasonably withheld

This should now prevent cases like *Gaskin* [38] from developing, where it was necessary to go to the ECHR to force the release of material relating to Gaskin's early life It is also another manifestation of proportionality

Vital interests – sch2 para4 – are life-threatening circumstances, and would affect health authorities, and local authorities, particularly in the case of 'notifiable' diseases, since the data subject might simply be too ill to give consent Significantly, the data subject is now entitled to receive a copy of the notification since they need to be able to exercise their right to ensure the accuracy of details given about them

We have already observed that MPs cannot expect to bypass consent, the same is essentially true for local authority elected members. The OIC, besides pointing out that elected members should feature as a class of data recipient in local authorities' notifications, identifies elected members as appearing in one of three roles

- as a member of the Council (such as a committee member)
- as a representative of the residents of the ward they were elected for
- as a representative of a political party

As a member of the council, the elected member is bound by the council's data protection policy, its notification, and is essentially on the same footing as an employee of the authority Proportionality is relevant: a member of a housing committee may attend a meeting which will decide whether to evict a tenant for rent arrears, say – and information may be shared with the member to facilitate this – but general access to housing department records (paper or computerised) would not be proportional or justified, and is therefore linked to DP Principle 2 regarding purpose Copies of information given to members under such circumstances are to be kept secure – and the member as an agent of the council, and the council itself – are responsible for this security

Even on ward work, the signed consent of the data subject would be prudent, as with the case of the MP, a proforma consent form might be a means of facilitating this with local authorities Nonetheless, it would need to be made clear that any personal information supplied were for the limited purpose of assisting the data subject and not for any other purpose The OIC guidance also states that noting requests by councillors (and by extension, MPs) for such information would be good practice

Disclosures of personal information for party political purposes may only be made with the explicit consent of the data subject There are only two exceptions

- for those data sets which the local authority is required to make public
- information that does not identify any living individual, but if anonymised information can be related to living individuals by comparing data (such as property data with the electoral roll) then this would occasion a breach of the DPA

Satisfying the requirements of data subject consent raises the practical issue of satisfying the data controller as to the identity of the data subject The example already mentioned regarding the bogus police caller suggests just how viciously regressive an identity argument can be, a plausibly reasonable amount of verification was undertaken, but even this proved to be inadequate None of the usual measures for establishing identity would be foolproof signatures can be forged, as can photographic ID cards Telephone enquiries, even when a reference number is asked for (such as a payer number), could be faked Security measures, to be seen as reasonable, also need to be proportional to the importance of the information held

In the exploration of the realities of compliance, the public are most likely to experience the effects of data protection and surveillance in relation to CCTV, the monitoring of nuisance – notably noise nuisance – and benefit fraud Once again, the reality of compliance with the underlying human rights, primarily Article 8, is secured by compliance with data protection law and good practice [39] Purpose – its clear establishment, and proportionality in conforming to it - is key; there has already been a challenge in *Regina v Brentwood Borough Council ex parte Peck* [40]

The essence of this case was that Mr Peck, suffering from depression, tried to kill himself in Brentwood town centre. Having been detected on CCTV, the police were summoned, Mr Peck was given medical assistance, and then taken home However, without Mr Peck's consent, the local authority released his images to the local press, and then to regional and national television Mr Peck complained successfully to the Broadcasting Standards Commission and the Independent Television Commission of

an unwarranted infringement of privacy Pre-HRA 1998, the High Court ruled that Mr Peck had no remedy against Brentwood Borough Council – but before the ECHR, it might well be a different matter.

It would seem perfectly in keeping with DP Principle 2 that CCTV images might be used in court but not for the entertainment of the public without the consent of those depicted, only for the purpose of obtaining public assistance for a police enquiry would it be likely that such images could be broadcast. Mere media prurience could not be sufficient – it would not fall within the legal *purpose* of CCTV, prevention or detection of crime would And the OIC Code of Practice makes this clear in Standard 6 relating to access to, and disclosure of, images to third parties, if images are to be made more widely available an appropriately designated member of staff must make that decision and the reason should be documented Disclosure to the media other than for a documented purpose should involve the disguising or blurring of individuals to prevent ready identification

The OIC has recognised the need to make progress on 'joined-up' information arrangements to facilitate the modernisation agenda of government, and particularly e-government It is one of the partners in the Cabinet Office Performance and Innovation Unit (PIU) study on the sharing of data within government and the promotion of personal privacy [41] The tension that exists between data sharing, for greater service efficiency and preventing/reducing crime, and the requirements of privacy, is explicitly acknowledged by the PIU It is the intention that the PIU project should establish a government-wide framework (or, indeed, frameworks) for the management of data sharing

One of the areas this has focused attention upon is the quality of the data used in data matching, where this is legal – and the OIC Annual Report released in June 2001 raises this matter in relation to the Police National Computer (PNC) – and the Association of Chief Police Officers' compliance strategy to deal with the shortcomings, which has yet to be fully implemented More worryingly, the OIC Annual Report describes the situation as "critical" where the new Criminal Records Bureau (CRB) is concerned The criminal conviction certificate system this will create will impinge upon employment decisions where these take CRB 'disclosures' (as they

will be termed) into account The Information Commissioner herself (when she was still known as the Data Protection Commissioner) expressed her dissatisfaction with the quality of PNC information, and made the important point about those performing the data entry. they should understand the value of what their work will produce [42]

A further concern is that the recommendation of the Masefield Scrutiny into the Criminal Justice System in 1995 – that courts should input data on court results directly onto the PNC rather than the police, to save time and enhance data quality – had still not been effected by the time of the Home Office 2nd Report, and was again recommended This was first put forward in the Home Affairs Committee Report *Criminal Records* in 1990, so more than a decade has elapsed from the first instance of recommendation This scarcely inspires confidence in central government

Just as worrying is the use of Capita – under a Public-Private Partnership arrangement – for the operation of the CRB, their record in local government for the operation of housing benefit systems has been the subject of controversy [43] Following the experience of the problems with the Siemens contract for the Immigration and Nationality Directorate's casework project, the Home Affairs 2nd Report recommends that the CRB Capita project be subject to piloting before full implementation The CRB will also be required to monitor the number of complaints it receives about certificates being incorrect, as part of the process of improving the quality of data from the PNC

The compliance which the OIC seeks also operates within a broader international framework of law and regulatory activity One of the arrangements with implications for future relations with internet service providers, for example, is the US 'Safe Harbor' scheme, designed to provide a level of protection for transfers of personal data to the US from the EU member states which meets European data protection requirements The arrangement, adopted on 26 July 2000, came into force in November 2000

Concerns about crime are refocused by the international dimension The Europol Convention [44] established a data protection Joint Supervising Body (JSB) through which the OIC has taken an active part in auditing Europol The OIC also attends the

Schengen Data Protection Common Control Authority as an observer, now that the UK participates in the Schengen arrangements for the sharing of police data Significantly, there is now a single secretariat for the JSB, the Schengen Information System Common Control Authority, and the Customs Information System Joint Supervising Authority, an example of joined-up thinking at a European level

The OIC also actively supports the approach of integrating formal law and self-regulation in the implementation of data protection law, and to this end, the OIC participates in the European Standards bodies' Project Steering Group (the project being set up at the behest of the European Commission), examining the possible role in implementing data protection directives that standards activity might play The OIC takes the view that data protection is likely to be more successful if those required to comply with the law take ownership of the problem and produce good practice solutions – technical or managerial – which can command wide acceptance This approach might well help to forestall laborious or cumbersome standards, by building on the practical knowledge gained by those working with the reality of data protection

In this examination of compliance matters, we have seen a number of key issues

- legal constraints on privacy in the interests of law enforcement
- allowance for free speech – such as journalism, research
- the mechanisms of national security
- misuse of sources of personal information
- the practical reality of compliance for public authorities
- the national and international roles of the OIC

These have all been engaged by the passage of the Anti-terrorism, Crime and Security Bill through Parliament after 11 September 2001, on its route to becoming an Act in December 2001.

The nub of the legitimacy of interference with data subject privacy is the reasonableness of the 'trigger point' for interference, which is obviously connected

with proportionality, since if the interference is proportional to the need, it is (essentially) reasonable We have already seen that Article 8 ECHR admits of interference with privacy where this is necessary in a democratic society, the prevention and detection of crime is plainly necessary, and terrorism is a particularly destabilising form of crime Having acknowledged the ground of the argument leading to the Act, does the Act embody a reasonable and realistic response to the problem? Balance is important, since part of the democratic society in whose name we are seeking powers to interfere with privacy for consists in that private life which we want to protect against the depredations of terrorists

The essence of the information disclosure clauses of the Bill [45] is related to crimes and the prosecution of offenders

which may relate directly or indirectly to national security [46]

and the extension of disclosure powers relates to

information which directly or indirectly relates to a risk to national security or to a terrorist [47]

This second matter was the key stumbling block in the case of the information clauses The Opposition parties and others – notably in the House of Lords – sought a clause containing the words above, while the Government sought something broader The problem, of course, in investigations is the point at which the 'triggering off' of the investigation with regard to terrorism really begins

The Opposition (Conservative and Liberal Democrat) advanced the view that there had to be a suspicion that there was a direct or indirect link with terrorism for information about another type of crime – say credit card fraud, which is often connected to terrorist funding – to be passed on to the authorities dealing with terrorism The Shadow Home Secretary [48] emphasised that, to trigger the proposed amendment to the wide power the Government suggested, authorities needed merely to suspect that a person was indirectly linked to terrorism The objection to the Government position was essentially one of proportionality, to prevent 'trawling' over data, where a person might have committed a minor offence, even in another country

The Home Secretary had accepted [49] that those elements of data that "someone could second-guess" as being as relevant to terrorists should be separated out from those to do with organised criminals and others, because the matter related to retention of data – this was the Liberal Democrat amendment to Part 11 of the Bill – and as the Home Secretary pointed out, as a result of this amendment

> we will have to retain the data, so that it can be accessed to test out whether the intelligence services are right in believing that it is relevant in tackling terrorists

or the whole Bill would be lost under Parliamentary rules

In the House of Lords, Lord Rooker, for the Government, pointed out that the proposed Lords amendment number 5 would have made it more difficult for public authorities to disclose potentially vital information; not being experts in terrorism, they would not be able to satisfy themselves that information was linked, even indirectly, to terrorism The difficulty, exposed by the Lords, was that there was no escaping the disingenuousness of the Government's position, since the issue arose in essentially two ways

Either (1) a public authority would be asked for information by police and security services re individuals (whom these services suspected of terrorism),
or (2) a public authority would suspect even an indirect link to terrorism – and could share the data with the relevant security authority

On what other ground could any meaningful action take place? If terrorism or a threat to national security were not even indirectly suspected there would be no action initiated, either something is suspected or not, and the draft clauses Part 3 s17(3-5) allowed disclosure for such suspicions, so what was the need for a broader disclosure power?

Lord Rooker made the following point [50]

The Inland Revenue has previously been unable to disclose to the police that a drug dealer was citing drug dealing on his tax returns I read that slowly because I gulped this morning when I read it That could prove to be a vital piece of intelligence but it cannot be passed over under your Lordships' amendment because the Inland Revenue has no idea that the drugs are linked to terrorism

One might say· except when they suspect even an indirect link? Lord Thomas of Gresford intervened to restore the original amendment [51], pointing out that it is for the police to make connections with, say, drug information, and thus for them, or the security services, to make a request under the amendment as suggested in (1) above If the Government were to have its way here, there is the distinct possibility that the security services and the police could be swamped with information There is also the issue of responsibility, Lord Thomas of Gresford continued [52]

When he introduced his amendment, the noble Lord, Lord Rooker, said that public authorities are not experts in terrorism As they are not experts in terrorism, why, without any guidance from Parliament, is this burden of determining what is proportionate to what is asked of them being thrust upon them?

As we have previously observed, this placing of the burden of making the judgement on the public authority is already a feature of the HRA-DPA-FoIA regime Nonetheless, the Government got its amendment 5B in the Lords, which became s17(5) of the Act, since the Conservatives in the House of Lords did not ultimately press the point, but the Government could not be said to have really won the argument

Recognising the importance of protecting the foundations of our society has been a theme throughout this section regarding compliance, privacy, as an important good of a free society, is one of those foundations, which is why safeguarding it successfully against abuse should be one of our foremost political and legal concerns Assessing the coherence of the approach to these issues as they have developed in the UK will therefore be an important part of the subject matter of the next chapter, in the discussion

CHAPTER 4: DISCUSSION

In determining whether data subject privacy in the UK is well-formed, we must, as one of our first tasks, obtain a conception of privacy which is internally consistent In Chapter 2, we examined competing views of privacy and outlined some of the necessary elements of a practical statement of what would be required in ramifying the NCCL (now Liberty) definition Now it is time to set out the essential components of the ideal type of privacy

4.1. The ontology of privacy

Ontologically, we must begin with *persons*, without entering into any dualism of the mental and physical, and agreeing with Nozick to the extent that we refuse a superficial Platonism that would reify institutions above persons This makes persons prior to property rights (and property obligations) and natural persons prior to legal ones This provides a bulwark against overriding persons in the interest of a 'greater good' where society is elevated in moral (and political) status above persons We are not to be treated as property or *objects* of institutions Rather, we are *subjects* This also means that some aspects of persons are prior to proprietory relationships – we cannot treat others as means and we cannot be treated as means either, not even by ourselves, without compromising our moral-ontological status – without giving rise to a Kantian antinomy of reason, a moral self-contradiction This is a warning against self-publicity as a commodity, and may explain why this so often creates difficulties for those who indulge in it

Persons are ends in themselves, without the *dignity* of not being commodities, we are morally naked Loss of dignity involves loss of control of the person, and a diminution of personhood This is why loss of dignity can be so psychologically shattering, too much is revealed Privacy is therefore a key to dignity and control of the self, of the personal space the self inhabits But there must be freedom to realise privacy, it requires autonomy to be 'cashable' For data subjects – persons in the context of informational privacy – this means legal entitlement of control over one's own affairs and control over the disposal of information about ourselves This autonomy – a freedom from control by others, and a freedom for the self to take control of its own affairs – is an important liberty, for no really mature action is

possible without it Even though it is a positive right in law, via the DPA 1998 in Britain, it is overall a negative liberty (in a Berlinian sense) since it involves the freedom from state control over parts of one's personal life. Between the citizens of normal intelligence and rationality, there needs to be an equality of this liberty It is equally clear that this equality of status is not itself liberty, we could all just as easily equally be slaves

The positive aspect of this liberty is clearly limited – the liberty of the privacy of the data subject (and as a morally agentive person in general) is a positive freedom to pursue one's own projects, but not one to impose those projects teleologically on others This is the point at which the tension between equality and partiality makes itself felt, and if we are not to have a society of individuals and groups endlessly at war with one another, this requires a controlling framework of law – and a culture of values motivating a general acceptance of this law – which both requires and allows tolerance of project-diversity

The account Nagel [1] gives of this is more plausible than the very theoretical 'original position' advanced by Rawls [2] In both cases, however, there is an acceptance of the key point that this toleration requires a higher-order impartiality, there is a difference between the values one can appeal to in conducting one's own life and those one can appeal to in the exercise of political power. The rules to be held in common for the regulation of public activity and behaviour – including interpersonal behaviour – are a more restricted set than those one could use purely in one's private life This is why Nagel rules out Type 4 coercion, because we cannot enforce complete value-conformity for Berlinian reasons. The tension between the impersonal and the partial in relation to public rules – law – cannot itself simply be bridged by making more such rules, even with deterrent punishments. We need to recognise the likeness of others to ourselves, and to confer the right (of privacy, or whatever it is) upon them In short, there must be *reciprocity*

Individual rules for conduct are not enough, there must be universalisable ones for public conduct, that are categorically imperatival Reciprocity toward others means equality of treatment, and must, if we recognise the importance of persons, mean a reciprocal liberty of privacy and dignity But this also cannot simply mean a

reciprocity of rights, that would only mean a balance-of-power-like bargaining between individuals, which we have rejected, along Nagelian lines. There must also be a reciprocity of the obligation or *duty* to confer rights, not just a reciprocity of the right to receive them

If rights are not expressed in the other-directed form of duties – to confer rights upon others – then there is always the risk of moral solipsism and selfishness The conception of rights in the other-directed form, however, requires the moral imagination to perceive others as moral agents It also means the others must also accept responsibility for their actions, as agentive moral subjects, rather than passive moral objects A purely self-directed conception of rights is going to be vitiated by selfishness To expect rights without other-directed reciprocity to deliver equality and liberty (including privacy) is another antinomy of reason

Klug [3] (among others) sees the UDHR-ECHR-HRA-DPA-FoIA framework as a higher-order framework of law of the kind we have been discussing. Certainly, on this kind of interpretation, the law is seen as being coherent, or 'joined-up' in current political parlance And such a legal regime also possesses another important characteristic – which we explored earlier – that of *proportionality* A basic requirement of that universalisability of our law is that it is logically economical and rational – but at the same time, that it is effective These are all parts of proportionality Part of the jurisprudence now required to be considered by British courts after the advent of the HRA 1998 is the balancing of rights, and this balancing is explicitly now part of the legal process via Articles 17 and 18 of the ECHR The danger is that, if the background conception of these rights is simply selfish, then those whose rights are balanced take away from the exercise no real sense of their obligations to others, no sense of mutuality.

Reciprocity alone can achieve a substantial balancing of rights Without it, the judicial consideration of public order and public safety concerns in relation to the balancing of rights is mere exhortation or sloganeering.

Klug's speaking of 'responsible rights' acknowledges that the key issue is that others have rights, but it is scarcely sufficient that the balancing of them is a matter only for

courts and public authorities (and to a lesser extent, private organisations) We need to do more than merely hope that reciprocity is going on (somewhere), that it is not going on nearly as much as we need is evinced by the large rise in crime over the period since the end of the Second World War The emphasis on rights – particularly against the agencies of the state – seems to have promoted an instrumental view of rights which does not encourage one to believe that there is much conceiving of rights as other-directed If the 'third wave' only offers individuals remedy against public authorities and organisations, and against other individuals by 'horizontal effect', and encourages individuals to leave any thoughts of the rights of others to the balancing by a judge, then this looks too much like an invitation to a litigious war of all against all, encouraged by supportive pressure groups with their own political agendas

This might seem to have taken us away from the legal consideration of data protection, but if it rests upon unsatisfactory foundations it will protect privacy only superficially Privacy is not just a matter of people not knowing one's business, the NCCL definition, as we have sought to extend it, recognises the importance of physical security to privacy

A thorough approach to privacy is not separable from the broader question of what sort of society we wish to live in, since if individuals are encouraged to claim rights without any sense of mutual obligation to securing the rights of others, it would not be surprising to find a narrowing of social sympathies leading to an increase in anti-social and criminal behaviour, and a selfish, instrumental attitude to the law – all phenomena observed in increase over the post-war period A political and legal environment that conduces to such moral solipsism is unlikely to be able to guarantee much domestic privacy or public safety; the data subject needs to be able to protect his personal information and private space from burglary and arson and his physical person from mugging just as much as from illegal forms of data processing by a public authority or private organisation We need to be thinking of a culture of privacy because informational and physical privacy are not really separable

Recognising the continuous nature of privacy, from the informational to the physical, itself entails further ontological priorities The distinction between the personal and the impersonal spoken of earlier led us to conclude that things are fungible because

they are impersonal, not the other way round The significance of personal data meant something close to absolute possessory entitlement of its use and disposal However, the connection between informational and physical privacy suggests that there is an important distinction to be made between trespass in a personalised space like a dwelling and someone walking across an open field A house burglar can breach our informational privacy just as much as the virtual burglary of a computer hacker The theft of industrial secrets is an equivalent for legal persons

In seeking to be proportional as to trespass over property, we need to be careful that no juridical route is created which opens any gap in the legal safeguards as to physical privacy which themselves are protecting informational privacy Self-invasion of privacy through publicity is another route, which nowadays is an increasingly broad highway to loss of dignity

It is instructive – not least for the consideration of any attempt to characterise obligation in law – to note that, in law, a breach of confidence is a breach of an obligation of confidence owed to another, whereas privacy, in respect of information at least, extends to the nature of the information itself, not just to the process of managing it Privacy is also to be kept separate from defamation and 'false light' issues; an appearance in a defamation case could breach privacy, but defamation is about reputation, not privacy *per se*

Cross-cutting privacy, partiality and equality is the question of interest Within the ECHR, this is characterised as the Article 10 right to receive and impart information We have already considered the extension of the notion of interest to cover the two aspects of public interest, which can be summarised as *openness* and *closure*, relating to information and protection Public interest in information – openness – is realised currently in the exempt journalistic and artistic purposes recognised in the DPA 1998, in public authorities' information, which will come via FoIA 2000, and via PIDA, with public interest disclosure Public interest in protection – closure – is recognised in existing law by the CDA 1998, within the controls of the DPA 1998 itself (and hence via s40 of the FoIA), and links to CDA 1998 via s115 of that Act through information-sharing protocols There are then further protections and routes to investigation of criminal activities in anti-terrorism legislation

Article 8 ECHR could be said to embody private interest, the freedom to pursue Williamsian projects insofar as these are not incompatible with the kind of higher-order values which we have discussed That these private interests must not be incompatible with higher-order values is evinced in Article 8(2), there could not be valid racist, murderous, or paedophile projects, for instance, since these would be inherently incompatible with a categorical imperative

The problem, as we have already discovered, is that the existence of reciprocity is presupposed, but with little succour, by the HRA framework, which only goes so far as to acknowledge the balancing of rights The emphasis on rights provides no means of reinforcing the message that rights cannot operate without the obligation on each to allow the expression of the rights of others, without which talk of rights is empty Reciprocity is missing from the legal framework

Moreover, even if it were possible to underpin 'third wave' rights to create a genuine legal and moral cosmopolitanism, with a legally-supported reciprocity, the whole edifice thus created needs political will to make it work Kant's view [4], that the only thing that is good without qualification is a good will is apposite here (as is the implied corollary, that the only thing which is bad without qualification is a bad will) Without this good will, there might be compliance with the letter of the law in a technical and instrumental way, by organisations, but that would leave so much untouched – there needs to be attitudinal change

The case of *Campbell v MGN Ltd* [5] exemplifies the current state of the development of attitudes to privacy The case demonstrates that there is now legal machinery to obtain at least a practical degree of compliance by organisations, but the reaction of the editor of the newspaper – who disingenuously reported the outcome as a threat to press freedom – makes one question the existence of any real internalisation of the values upon which data protection law is purportedly predicated The claimant accepted that the newspaper was entitled to publish the fact that she was a drug addict contrary to her public statements, but the newspaper was not entitled to reveal the details of her Narcotics Anonymous treatment in such a way as to identify the location of her treatment which could open her up to personal physical risk (and indeed for

others using the same facility) The ruling was that the details of her treatment were sensitive personal data, and Article 10 is not an unqualified right, as Article 10(2) requires respect for privacy and restraint on the newspaper was hence considered to be proportional The newspaper could therefore expose her hypocrisy, but not so as to risk her physical or mental health, the details being protected as sensitive personal data within Sch3, DPA 1998. Rights have been balanced, but would it not have been better if a deeper understanding of the underlying matter of privacy had been exhibited by the press?

Following the Court of Appeal judgement [6] this balance has been shifted back to the favour of the press the cost of self-publicity has proven to be high. The Court of Appeal decided that the photographs of the street scene did not convey confidential information, and therefore there was no case to answer under DPA 1998 – the journalistic exemption in s32 was activated This itself was linked to Article 10(1) of the HRA 1998

Lasch [7] has commented.

> Liberals have always taken the position that democracy can dispense with civic virtue According to this way of thinking, it is liberal institutions, not the character of citizens, that make democracy work

While this charge could not be levelled at Kant, nor at Mill (for whom liberty was to provide the conditions to foster character), it does seem to characterise the naive optimism of the UDHR and the ECHR Too much has been taken for granted; one only has to see how many of the member states of the UN do not meet the standards of the UDHR It is also difficult not to conclude that in the West, the shift of emphasis – notably in law and education - from the inculcation of moral character to the promotion of human rights has seen the rise of several generations in whom there are fewer internal psychological controls preventing them from acting without reciprocity. The rights approach to law has not been ideologically neutral or without social consequences and the higher-order values from which the rights are claimed to have been derived do not appear to have rooted themselves deeply

We have therefore an instrumental approach to rights – action is, in Weberian terms, *zweckrational* What is needed is a proper appreciation of the values – categorically-imperatival ones – so that action is *wertrational*, or *autonomous* That autonomy which went with privacy is also inseparable from the adult moral person exhibiting moral character, who can accept their moral obligations to others And without that, we will have very little real *society* Failure to nurture reciprocity breaks the chain of moral-ontological commitments which enables successful civil society to thrive This raises the spectre once again of the fate of the 1960 Canadian Bill of Rights, or worse, in our case, if the legal machinery to protect privacy is seen not to be delivering real physical privacy, this machinery will not command any allegiance, and consequently, have no political legitimacy The political 'die-back' from this, if it were to overtake the 'third wave'rights approach that Britain appears to have embarked upon (along with the EU), could poison the political environment for any kind of cosmopolitanism for a considerable period

The cultural dissonance that might well flow from the advocacy of rights without a real concern for reciprocal obligations can be interesting for those who do not have to live with its consequences in terms of anti-social behaviour and crime, or pick up the pieces, unlike public authorities, and those who work in them, who do Value-pluralism in terms of personal projects must ultimately be congruent with some sense of what is – and what is not – ethically, politically, and socially tolerable in the public domain The higher-order framework of values must be realised in some public value-consensus

4.2. Truth and consequences

Privacy becomes a practical concern once we enter into the matter of compliance with the law as it currently exists, rather than as it might become. The differing regimes for compliance regarding time-limits in FoIA and, via s40, DPA, for personal information, are scarcely helpful, and one wonders if those who drew up the legislation really believe that all those who work in public authorities are genuinely and purposefully unhelpful If 20 working days is the deadline for requests – there exists a mechanism for extending this to allow for compliance where a qualified exemption applies, where a public interest test is necessary (such as would occur if

personal information were involved which could require partial disclosure and partial removal) – and data protection requests take up to 40 days – would it not have made more sense to set the *maximum* time at the same limit, while emphasising, along with Wadham *et al* [8] that the compliance with s1(1) FoIA should take place "promptly"?

Where information – personal or non-personal – can be given promptly, then it should be given, the time limit is a maximum, not an optimum. If the *maximum* were set the same for both classes or types of information, then the same regime, including the same extensions of time, could be made to apply. This would cut through some of the complexity of the legislative machinery, and help to join up the information legislation to embrace the continuum of information. It would also enable the OIC to look beyond the matter of timetables to the essence of information law – in the first instance, the 'giving of further effect' to Article 8 with regard to privacy and personal data, and to Article 10 with regard to freedom of thought and expression and non-personal data Parliament's linking of the freedom of information and protection of personal information aspects under the one Information Commissioner – to avoid both conflicts of interpretation, and roles, where the two functions exist as separate posts – would then have greater finesse. The substantive matter of the tension between privacy and public interest, the right to privacy and the right to receive and impart information, would be brought into clearer focus with the simplification of the machinery

The issue also of *responsibility* could also be more readily addressed, it is already explicitly listed in Article 10(2) Not merely do the responsibilities of public authorities need to be overseen, but the OIC could focus on the responsibilities of individuals – the policing of vexatious requests is important, as is the policing of frankly tendentious ones, where individuals try to obtain personal data about others either through the data protection route, or by attempting to pressure public authorities via qualified exemptions into revealing some personal or confidential information on the dangerous borderline of public interest

This leads on to the matter of the public interest test itself It seems a dangerous invitation to consequentialism, a game of 'consequentialist roulette' for public authorities The test as presented by the Act creates pressure to comply instrumentally

with the law, it will simply lead to a process where public authorities will seek to avoid getting sued The test is going to become an exercise in trying to work out which consequences will mean the quietest life, and gearing actions to produce this result Public interest will become whatever avoids prosecution This will make the process a purely utilitarian one, where decisions will become a quantitative calculus of consequences, but the penalty will be that it makes those decisions morally vacuous, if there is to be no further role for judgement.

To be of any use, a public interest test must allow thinking about the people who will be affected by the release of the information, and think about them as persons who are ends in themselves This will require moral imagination to understand the implications for individuals as persons like one's self The problem for the law is that this way of expressing the matter may well run counter to the FoIA presumption of publishing rather than not, where interest is otherwise balanced This public interest test is a specific FoIA manifestation of third-party effects The *Wakefield* case [9] is notably one where information which has been in the public domain will actually need to be more restricted, despite FoIA, because of DPA and Article 8

There is a further connection to common law confidentiality, particularly involving legal persons there might well be confidential data relating to legal persons entwined with data relating to an FoIA request S30(2)(b) FoIA exemption only applies to information obtained in confidence in relation to investigations and criminal proceedings S41 exempts information if its disclosure would constitute a breach of confidence actionable by the person supplying it (including a legal person) Trade secrets and information the release of which would prejudice commercial interests are also exempt This involves another round of consequentialist roulette where public authorities have to estimate whether release is or is not likely to be actionable as a breach of confidence and hope ultimately that they have made the right choice

The public interest test might simply be better conceived of deontologically – as a duty, upon bodies charged with providing the public with information, to protect personal privacy and confidentiality, and to define these areas The result would then be to permit other information not thus exempted to be made public FoIA starts the other way around – presuming openness in s1(1) and then trying to exempt bits

Personal data as a category does not appear until s40. It would have been better to have started here, working out to the penumbra of confidentiality and relations to legal persons, until much less ambiguously public-interest information was reached This is unlikely to satisfy the freedom-of-information liberal purists, but it might prove a more practical proposition, and more robust to challenge over what is public in the longer run Coupled with the earlier observation about a common set of rules for personal and non-personal data, this ought to give greater coherence and less bureaucratic apparatus, where there is already a single Information Commissioner and Commission

This line of argument cuts across that presented by Cornford [10], who is pessimistic about the chances of FoIA 2000 delivering real freedom of information, even with s1(1) and s2 in place to create the right to obtain information, and the presumption in favour of disclosure in the public interest His conclusion is that the complexity of the interactions of the legal machinery of the Act itself will enable governments (the argument he gives is essentially about central government) to avoid having to give the same level of access as foreign FoI regimes It should be said that the OIC has made it plain – to local government at least – that there will be a clear presumption in favour of disclosure, that exemptions will be treated narrowly, and that a comprehensive publication scheme is advisable, as a means of reducing the number of complex requests We can agree with Cornford about the complexity of the Act's workings, but the remedy is beyond the scope of the rights approach, since this sets up privacy and openness in opposition, to be 'balanced', rather than seeing the resolution of the tension by the proper consideration of privacy and confidentiality, and then working out to public information, in a systematic consideration of interest

To realise the rights of private citizens and private legal persons – as well as their obligations – what freedom of information must essentially be for is to provide for *informed* privacy, since this is the only state of privacy properly congruent with autonomy. For legal persons, this is realised in a state of informed confidentiality. This naturally raises the questions of the quality and quantity of the information to be made available

FoIA 2000 allows public authorities to refer requestors to information already published if this exists There is a danger of this becoming a vast public relations exercise, referring requestors to a body of statistical material which is ostensibly useful, but which is theory-laden with assumptions driven by government regulations and conventions, as appear in, for example, Best Value indicators, Housing Investment Programme and Chartered Institute of Public Finance and Accountancy (CIPFA) statistical returns. These are rich sources of public information providing that the definitions are understood – and these are often modified from year to year The rebasing of national crime statistics in 1998 prevents direct comparison with those from earlier years – and the basket of goods from which the Retail Price Index is derived also changes over time Information is not necessarily simply neutral; it exists in a charged political environment.

Worse though, within the FoIA provision for publication schemes, legal destruction schedules are likely to mean the destroying of material that has interesting content, but the preservation of officially-sanctioned anodyne material The rise of electronic storage and retrieval systems – of which more later – and the destruction of paper, contributes with the matter of enforceable document lifecycles to a considerable risk of information poverty in the future

We seem to have a nexus of risks, therefore, to obtaining an informed, meaningful privacy for the citizen, for it is now clear that we are some way off from having realised in Britain a well-formed conception and practice of privacy Privacy is at risk from too narrow a legal conception of what is required to protect and sustain it, and the attention to responsibilities rather than merely to rights is still too much like lip service What might be thought of as joined-up privacy, the explicit linking of informational privacy and physical privacy, even though it was a feature of the NCCL proposal, is still not realised in English law It is also clear that the freedom of information path that has been embarked upon will not necessarily make the autonomous private data subject significantly better informed or better able to be informed, because of the quality of the information which is likely to be made available Not merely is government information often theory-laden with political initiative, but journalism seldom serves no agenda at all

These issues – the realisation of meaningful privacy and the mechanisms of compliance to enable this delivery – are of more than merely academic or localised interest. The deadline for the Government's e-government target – 2005 – is approaching and much of the Government's political credibility has been staked on improvements in public sector services, closely bound up with electronic delivery and new forms of information processing The maxim 'say once, tell many' sets out what would be the Government's ideal, and it makes a slick phrase, but, as we have already seen with council tax data, the law restricts its use, and the OIC has taken a very firm line in protecting privacy, rather than promoting bureaucratic convenience Even consent clauses must not be too general, there has to be purpose, required by the data protection principles, and this must not be so general as to mean anything

The Performance and Innovation Unit (PIU) of the Cabinet Office has published its report [11] concerning privacy and data-sharing, containing proposals for increased use of personal data across administrative boundaries to deliver better public services Interestingly, the Report acknowledges that public concern about privacy is on the rise [12], but it is significant that many of the factors identified as 'drivers' for this increased sensitivity are linked to heightened awareness of physical privacy and personal security The rise in ex-directory telephone numbers and concerns about private-sector organisations' use of personal data such as ISPs tracking use of the Internet and using this knowledge for commercial gain are mentioned What has been identified in the Report [13] are the concerns about data processing which are common to public and private sector organisations

- unauthorised access to personal information
- unauthorised informal disclosure of personal information
- errors in data-handling
- infection with inaccurate data
- misidentification
- unjust inference (making decisions unfairly based on inferences from matched data)
- use of 'soft' data (such as professionals' opinions or subjective assessments of individuals)

The solution the Government wishes to promote so far as customer services are concerned is the private sector model of call centres (said without irony) [14]

services can be tailored to meet the needs of the individual client

NHS Direct is quoted as an "innovative" example, and [15] will be developed further to include patient access to electronic personal records One hopes that these are more secure than the online Inland Revenue service, where other people's tax details could be accessed With the data-sharing gateways created by the Anti-terrorism, Crime and Security Act 2001 (amongst others) and the general idea of technological fixes to enable greater data-sharing, all of the identified points of public concern over data use are engaged

Tucked away [16] in the Report are the words·

Citizens also have responsibilities, for example to provide accurate data, not commit fraud or other criminal activity, respect civil judgments, and so on

This would be more convincing if information law contained some real penalties for breaching these responsibilities, s55 and s56 of the DPA do not cover giving false or misleading information

At 5 12 of the Report, it is noted that there is a risk that the public sector is not making the most of technological opportunities, appropriate technology, of course, requires appropriate budgets

Overcoming public mistrust of public-sector use of personal data is a key aim of the Report To this end, it is intended to consult on a Draft Public Services Trust Charter, which contains the following [17]

Your information is only processed without your knowledge where this is necessary for purposes such as national security, public safety, statistical analysis, the protection of the economy, the prevention of crime and disorder, the protection of health or morals, or the protection of the rights and freedoms of others

The Draft Charter explicitly links these with the terms of the DPA 1998, and to that extent would, if implemented, help to clarify the scope of non-consensual processing However, the earlier concern in the Report with bureaucracy is glossed over with the Recommendation 1 at 6 18 of the Report

All public sector organisations should look to embody these principles in service-level privacy statements *describing precisely in each case* how personal information will be shared each service-level privacy statement will need to be embodied in working-level codes of practice and information sharing protocols, themselves underpinned by management guidance These should be made publicly available

This would be funny if it were not so serious, or self-satirising Recommendation 3 [18] suggests the consideration of new performance targets and indicators to measure all of this What, then, happened to cutting

as much of the administrative red-tape and costs as possible

at 5 11?

If the metarules of a data-processing trust charter are genuinely metarules, they necessarily apply to all data processing in the public sector. An Appendix of the affected areas for each case ought then to suffice Logical parsimony of this kind is preferable to the legal prolixity of endless Codes of Practice which implies that the primary legislation is lacking in clarity

More practically, the matter of data quality is addressed Recommendation 9 [19] suggests the introduction of standards for recording common items of data, and the Office of the e-Envoy should give high priority to implementing the Data Standards Catalogue of standardised data fields, Recommendation 10 charges the Lord Chancellor's Department in conjunction with the PRO with developing and disseminating model data-sharing protocols and codes of practice This last point will help, but more streamlining of the regulatory framework would be better

One pathway to resolving the issue of public-sector resources and the crossing of organisational boundaries would be the completion of unitary local government in England This would reduce the need to cross boundaries between authorities, because most functions requiring a heavy use of personal data would be within the ringfence of a single authority; this would reduce the need for protocols by reducing the number of data controllers and the number of 'partners' It would also create economies of scale in providing public services which should help to provide more resources for implementing changes to processes However, the building-in of privacy into processes is salient [20] but does not acknowledge the problem of local authority senior management taking too reductive an approach to systems, and failing to see the holism of privacy, data protection and freedom of information Better training for information management professional is proposed, though, via the Centre for Management and Policy Studies, drawing on the best practice of bodies such as the PRO, and the creation of Chief Knowledge Officers at board level would help, and within a unitary framework, they would be more likely to have the resources to go along with the responsibility

A greater help with consistency of decision-making in relation to privacy is the suggestion [21] of an Analytical Framework which provides a context within which Privacy Impact Assessments (PIAs) – already used in Canada and New Zealand – will allow new policies to be assessed for privacy risks, costs and benefits systematically These processes – applied realistically – should be of practical benefit to the 'foot soldiers' in local authorities and other public-sector bodies

Chapter 10 of the Report recognises the problems of the legal framework, the restraint on sharing Council Tax data in the LGFA 1992 is explicitly acknowledged Data-sharing powers – in the specific case of the Department of Work and Pensions – are highlighted, being currently spread over eight Acts of Parliament Fundamental guidance on data-sharing in relation to the DPA is to be developed by the Lord Chancellor's Department in response to the problems of the current legal framework

So much, however, is unaddressed in the PIU Report The Government is shown making assumptions about privacy which have the incoherence of being unarticulated, there is no satisfactory attempt to set out what privacy means The Report, as a

statement for the medium term future for public authorities, does not take proper account of the ontological connection of freedom of information and data protection matters, the 'continuum of information' is the key to unlocking the solution to linking them properly, because this joins them systematically and logically This linkage naturally relates privacy and openness, since these are both manifestations of *interest*, but this would require attributing appropriate weight to the conception of the private autonomous citizen as the key player in civil society, and challenging assumptions about the citizen as consumer

Raab [22], as one of those involved in the consultations for the Report, has recognised that the technocratic approach is inadequate to protect privacy, and has pointed out that privacy needs to be seen as a public good He has also pointed out that the concept of *balance* between privacy and the organisational benefits of data sharing is misleading, as the two issues are essentially incommensurable [23] Understanding the correct relationship arising out of interest, that privacy and openness are aspects of persons – the private and public faces, as it were – means that the balancing-of-rights approach captures the distinction wrongly, because it treats the manifestations of interest as only contingently, rather than fundamentally, connected What Raab has characterised a number of times [24] as *steering* (as contrasted with 'balancing') arises naturally out of rules conceived of as other-directed duties, rather than competing rights, of citizens as moral agents, since privacy as a manifestation of interest is a prerequisite of any deliberations about information, rather than being seen as something we may (or may not) have a right to after the organisational and technical questions have been examined

The professionalism of those charged with ensuring that the handling of information does not infringe privacy would, on a 'steering' view, involve the moral imagination to recognise and prepare for the situations in which infringements might occur as part of the initial setting-up of any processing arrangements, drawing upon the reciprocity of recognising the rights of others as a duty It would also mean vigilance in promoting the values and attitudes of privacy protection, and establishing a reputation for trustworthiness, which would not merely be an exercise in having the right policy documents or mission statements Practitioners have to believe in and understand what they are doing, and more management systems are unlikely to add value to this,

indeed, more bureaucracy is likely to overload those working with the issues of information and privacy.

Raab [25] speaks of the importance of building a 'culture' of data protection, so that implementing the law

> becomes an integral part of standard operating procedures [26]

This is very much what is required, and the multiplication of codes of practice will add nothing to this culture, it is not more regulations which are required, so much as the right ones, and intelligence and integrity in the staff who operate according to them A clear conception of privacy – as a key interest of citizens – has to be seen as an essential driver of policy formation and legislation, including the regulations deriving from that legislation The rights approach, even with 'balancing' and Article 17 of the ECHR is not enough Joined-up privacy is still not realised and privacy is therefore not well-formed in law

The tenor of the Report is instrumental in a way which we have already concluded is inadequate The problems of unjust inference and misuse of soft data and unauthorised disclosure of personal information are ones of lack of professionalism, issues relating to human judgement. These cannot be fixed with a barrage of service-level privacy statements, codes of practice and guidance, and such an approach will do nothing to improve the public's view of, or trust in, public services Instead, there is a risk of engendering more cynicism about 'words on paper'. Better management training is a helpful suggestion, in respect of encouraging the exercise of better judgement, but it must challenge existing modes of professional discourse If it fails to overcome the reductionist prejudice to holistic thinking about privacy and the processes of its protection, it could actually be pernicious Furthermore, the proposed Analytical Framework and the PIA process need to be robustly concise for practical use

That the PIU Report is calling now for greater powers to create information-sharing gateways is a matter for some relief in terms of the prospect advanced by Rule in 1973 [27] for the growth of mass surveillance and control via data processing, but all

the arguments so far – including Raab – bear out the view advanced by Rule and others in 1980 [28] that the answer to the problems for privacy posed by technology is not going to be found simply in a procedural solution the matter is inescapably political It depends on our conception of what sort of society we want to live in, what sort of people we want to be, and what value and significance we place on privacy in this conception

One comes away from the Report feeling that the Government has been insufficiently critical of the e-commercial elite's view of the world that may come The view taken back in 1980 by Rule *et al* therefore remains salutary:

> The current erosion of faith in the prospects of growing human control represents a trend of major significance People are growing skeptical of more and more powerful technologies as solutions to problems of highly developed societies People need to hear it said that limitations on the scope of human intervention need not be antiscientific, but may simply reflect the humility required in planning for situations in which the stakes may grow very great indeed In short, we need a program for rational limits to the extension of "rational" human control [29]

The lack of 'progress' on the joining-up of information attested to by the desire for data-sharing gateways in the Report is therefore also an opportunity, even now, so far down the technological track from Rule in 1973, for taking a different approach to the matter of securing privacy, both informational and physical

S40 FoIA's embedding of DPA at least indicates a *prima facie* recognition of the continuum of information, as does the placing of both FoIA and DPA responsibilities under the OIC What is left, however, is the sense of something missing at the centre of the legislative framework, this lack having made possible the degree of fragmentation between different Acts The citizen as a consumer of services with rights does not fill the ontological void, a passive version of cosmopolitanism cannot sustain rights, as has been argued, and does not convince Reciprocity is needed to activate the rights by obliging individuals (including those acting singly or together as legal persons) to actually confer them on others There remains no conception of the private autonomous data subject as an agentive moral person which would have informed the process of legislative creation and bound the law, the citizen, and a common core of civic values into a culture of privacy.

CHAPTER 5: CONCLUSIONS

5.1. Prolegomena to future information and privacy laws.

It was seen at the end of the discussion in the previous chapter that progress in obtaining better protection for privacy was essentially a matter of, and for, politics It also depends on a particular set of choices in politics; the ontology of privacy that has been discussed constrains the path we can take if we value privacy as much as we claim to Privacy requires the rule of law, and the duty to respect the right of others to it Privacy, which makes for healthy civil society and healthy individuals, needs effective laws to safeguard it, and to be valued as a good to ensure the political culture to sustain it In the concluding remarks of Chapter 2, the ramified definition of privacy was set out, identifying the key features which need to be addressed in any analysis of it, but also with the recognition that the definition has to be placed within a deontological framework to be fully effective Such a definition forms an important list of the features of privacy which would have to be considered in any statutory legal protection of it These key features can be summarised

Solitude is not merely the right to have one's physical senses unmolested in any private place but also to freedom of thought and reflection, free from social pressure and the coercion of others

Intimacy is necessary for the maintenance of emotional and physical health

Anonymity is closely linked with the requirement of autonomy – the freedom of action of private persons in matters that concern themselves

Reserve includes freedom from psychological pressure and from physiological interference, including freedom from unwarranted scrutiny, and is therefore linked to solitude and autonomy

These first four aspects of privacy are all concerned with dignity, which takes us from the libertarian conception of the commercial and the rule of market forces, to fundamentals incommensurable with money

Privacy of personal information is a general requirement for confidentiality, which is the means by which the previous aspects of privacy can be realised

Reciprocity involves value-tolerance for others' private lives and religious beliefs, it also means that certain privacy rights must be qualified in public places, including workplaces, recognising that our behaviour is likely to vary in different social contexts, as a matter of different degrees of intimacy and solitude

Proportionality is connected to this reciprocity, recognising that reciprocity requires a sense of when and how much, entailing moral judgement

It was also seen in Chapter 2 that Nagel's realism about equality and partiality keeps us closer to Kant's own reasoning about ethics than Rawls' much more theoretical 'original position' argument, interesting though it is, and Nagel's 'agent-neutral' (rather than 'agent-relative') reasoning yields the 'higher-order' public ethics (rather than personal ethics) that liberals (including Klug) would be looking for The distinction in Kantian ethics between the internal realm and the external juridical realm which must be agent-neutral and provide universalisability in accordance with a categorical imperative is realised, but only with the corollary of duties upon moral agents to strive for agent-neutrality, rather than merely seeking rights

This is opposed to utilitarianism as a means of achieving a higher-order public ethical framework, and does not require the breaking of the links between personal and public morality which utilitarianism can lead to, which Williams has amply discussed [1], essentially, utilitarianism alienates public ethics from personal ones by putting too much emphasis on the collective, rather than on the individual as a social being, and on instrumental methods of decision-making This contributes to a centralising, bureaucratic, even utopian, approach to ethics, which can easily leave the individual citizen remote from those decisions made in the name of the people

Our argument is also opposed to that prevalent strain of thought which would ally utilitarian thinking with David Hume's poisonous dictum [2], that reason is, and ought only to be, the slave of the passions, which yields up the emotive instrumentalism of

the consumer society Duty to others is the only way to ensure that rights are other-directed, rather than being selfish, and this ontological ordering makes rights which are other-directed *active*, rather than merely being passively received and consumed by individuals from public authorities The danger is that of producing a sham 'soft' cosmopolitanism of rights, that will fail, and taint the political environment, hindering the creation of a genuine 'hard' cosmopolitanism of duties, as Kant envisaged, one which would actually deliver real human (other-directed) rights The first is content to sloganeer, the second actually requires moral actions, which would be basic duties on each citizen, not just on corporate public legal persons And one of these basic duties would be not infringing the privacy of others, conferring on others the right of quiet enjoyment Privacy is not just about informational privacy from the state, the emphasis (one might even say overemphasis) in the ECHR regarding the state is very much a product of the circumstances of its inception, out of the experiences of Nazi-controlled Europe, and of the Cold War world which followed A privacy law would protect privacy from all likely threats to it, but not against justifiable intrusion to prosecute criminal acts, or to expose them

This brings us back to the public and private faces of interest Our private autonomous citizen – the mainstay of a healthy civil society – has to be an informed citizen if they are to play their part in a democratic society. Interest is therefore continuous – 'joined-up' in current political parlance – and reflects the 'continuum of information' from private to public Simply embedding data protection rules in a Freedom of Information Act, as happens now, is not enough Also, making the exemptions from disclosure follow a logical sequence from personal to impersonal information, taking account of the interests of the citizen, from personal and national security to the need to be informed as an active and political being participating in a democratic society, should address the concerns of commentators like Cornford [3]

All of this entails the need for measures to promote the development of the private autonomous citizen We have heard much about his or her rights and entitlements from public authorities and organisations, but much less about his or her reciprocal duties to other citizens, or how these might be framed in law. The *Infringement of Privacy* paper [4] in 1993 raised the prospect of creating a statutory tort of infringement of privacy as a way of addressing privacy protection, but the advent of

the Human Rights Act in 1998 before such legislation was created has changed the nature of the legal landscape in which any future privacy law might operate This is due to the effects of access to the Convention Rights which are of European origin, and which have been interpreted in the purposive manner of the continental legal culture, shaping the jurisprudence of the European Court which may now be drawn upon in interpreting these rights in English courts.

There has been a traditional distinction made between the mode of English law - emphasising literalism of interpretation, the case law emphasis on form and precedent, and the adversarial system of courts – and continental European law – with purposiveness in interpretation, and an inquisitorial system of courts The civil law tradition in France has already yielded a privacy law English law has historically given no formal safeguards for privacy, preferring the 'organic' approach of common law and precedent Furthermore, any legal principles – like proportionality, or, indeed, reciprocity – enter via 'concrete' procedure and precedent, such as the *Wednesbury* rules [5], with legal principles tending to be known by the names of the key cases exemplifying them

It is salutary to note that this division between English and continental law is less firm than one is often led to believe Denning [6] argued for purposiveness in English law during a long legal career, eventually becoming Master of the Rolls. His views are instructive

> In the absence of [clarity in Acts of Parliament], when a defect appears, a judge cannot simply fold his hands and blame the draftsman He must set to work on the constructive task of finding the intention of Parliament, and he must do this not only from the language of the statute, but also from a consideration of the social conditions which gave rise to it, and of the mischief which it was passed to remedy, and then he must supplement the written word so as to give 'force and life' to the intention of the legislature [7]

Denning continues

> We do not sit here to pull the language of Parliament and of Ministers to pieces and make nonsense of it We sit here to find out the intention of Parliament and of Ministers and carry it out [8]

More intriguing still is the historical depth of the purposive approach in English legal history, Denning refers to remarks by Viscount Dilhorne in a case from 1978 [9], quoting Lord Coke

"It is now fashionable to talk of a purposive construction of a statute, but it has been recognised since the seventeenth century that it is the task of the judiciary in interpreting an Act to seek to interpret it "according to the intent of them that made it" (Coke 4 Inst 330)" [10]

Denning also points out that this has been an increasing feature of English law since the accession to the European Economic Community (now European Union) in 1972 This European purposiveness is known as the 'schematic and teleological' method of interpretation, by which judges go by the design or purpose lying behind the legislation, not by the literal meaning of the words, or by the grammatical structure of the sentence

Denning's conclusion is that

We should adopt such a construction as will "promote the general legislative purpose" underlying the provision [11]

This view suggests a general question 'what did the legislators mean and intend?' and judges should attempt to give effect to what they find to be the answer This avoids as far as is practicable what Kant objected to as 'judge-made' law, discussed by Rosen [12], but it also argues in favour of the greatest possible clarity in legislation in the first place, and careful deliberation on what the law is to apply to The emphasis is placed back on legislators, and the political process, judges should not have to remedy legal defects too often This line of argument provides English legal roots for what we might call 'pragmatic purposiveness', which would enable us to have home-grown legal principles such as reciprocity, as well as proportionality, while restricting interpretations that would strain the meanings of the words of legislation

The absence of a privacy law in the UK has led to recourse to the Convention Rights made accessible through the HRA 1998 Also, the protection of personal and sensitive personal data is enabled to an extent through the DPA 1998 The problem is not, as

Bainbridge *et al.* [13] suggest, that data protection is 'tilting at windmills', so much as data protection only addresses part of the problem of privacy, which only the formal recognition of the tortious nature of its infringement will cure Kant, as we have already mentioned, was opposed to what he saw as 'judge-made' law, and we have seen in the lengthy and expensive court battles over privacy via human rights legislation that it is an unsatisfactory means of securing proper protection for it A statutory safeguard, with legislative clarity, but with a duty to avoid abuse of the right, would provide the deontologically satisfactory solution

The evidence of the need is there staff of the Inland Revenue service [14] have been caught browsing through celebrity tax records, and there is evidence of malicious use of information, with such activities as selling information to outside organisations While there have been dismissals from the Inland Revenue following the most serious of these cases, it demonstrates that the emphasis on systems and procedures so strongly made in the PIU Report [15] does not touch the underlying question of the integrity of staff These are offences under the Data Protection Act 1998 and the Computer Misuse Act 1990, but the existence of these rules has had only a limited deterrent effect There is little sense of an internalisation of a value-culture of privacy – with a respect for others – which would underpin the law

However, it is unlikely that a political articulation of a culture of privacy of the kind suggested by Rule *et al* [16] will spring into life fully-formed The deeper social and legal changes needed to move the issue of privacy towards a coherent polity of respect for privacy, requirement for moral character, and a broader understanding of duty are likely to come only when the easier technical changes have been made These changes themselves should have the effect of modifying habits and might help to create the environment in which a culture of privacy could more easily grow These changes are also practically desirable in themselves

5.2. Conclusions forming recommendations

The conclusions about the current state of data subject privacy are of essentially two kinds

- those which relate to the general matter of privacy, and
- those which relate to the apparatus of existing information law

The first of these concerns the ontological void identified in the previous chapter, which has manifested itself in the insufficiency of existing protection for privacy It is, however, the second of these points which can be more easily addressed, as part of the modification of processes and habits of information law and its effects on data subject privacy

5.2.1. There should be harmonisation between the time limits for FoI and DP requests, and both should be in writing.

That personal information is recognised as being part of a continuum of information, both by being included in FoIA 2000 at s40, and by the subsuming of FoI and DP roles in one OIC is a sensible and practical state of affairs

However, we then have the perversity in FoI where the public do not have to identify an FoI request as such, and the public authority has to guess This is compounded by the difference in compliance times, and means running two separate bureaucratic regimes (which are largely expected to come out of existing staffing resources and budgets, thereby masking the cost) DP gives a maximum of 40 days, and FoI 20 working days (with a mechanism for extending this where a qualified exemption applies)

This cries out for rationalisation In Chapter 4, it was suggested that the period be harmonised One would be inclined to suggest 30 days, and an extension of time mechanism for qualified exemptions for FoI purposes, or third party consultations for both FoI and DP Again, the requirement in s1(1) FoIA 2000 to comply "promptly" would stand This harmonisation would enable the public interest decisions in FoI to be joined with the third party information release decision process in DP as one process, with one embracing code of practice

A subsidiary recommendation might allow us to go further

5.2.1.1. A future Information Act – linking FoI and DP concerns – would order the categories of information – from personal to non-personal – more logically.

This would show the absolutely exempt information, beginning with personal data in connection to FoI issues, and then moving to confidential information for legal persons, then to the qualified exemptions, working outwards to the types of information that would be almost never exempt It would also make the class-based and prejudice-based distinction explicit The two recommendations 5 2 1 and 5 2.1 1 together would enable much greater consistency of treatment for information processing, and even the proposal 5 2 1 taken singly would advance the prospect of genuinely 'joined-up' government

5.2.2. Data-sharing gateways should be created by an amendment to the DPA 1998.

The Annexes to the PIU Report [17], notably Annex A, point out that the gateways are necessary, since the 'indivisibility of the Crown' doctrine does not apply in the data-sharing area This relates back to the almost absolute possessory nature of the entitlement to the use and disposal of personal (and sensitive personal) data It is a manifestation of the data protection principles 2 and 3 regarding specificity of purpose and relevancy. This points to the ontological feature that consent is not transitive – or is only allowed to be so in a restricted way, with explicit controls by the data subject opting in Only where criminal activity is reasonably and justifiably suspected is this able to be overridden

A 48 of the Annexes considers whether the LGA 2000 via the power of local authorities to promote economic well-being, might be enough to establish a gateway for data-sharing, *prima facie*, the answer must be no – it cannot override specific prohibitions in other primary legislation

One would hope that any data-sharing gateway-making power would arise as an amendment to DPA 1998, since this would yoke it directly to the data protection principles and the categories of information and potential organisational partners listed within data protection notifications

These types of partners would be the objects of the data-sharing gateways, these would be activated by statutory instrument, adding to a schedule, with any statutory instrument being subject to the 'affirmative' procedure (under which there must be a vote in favour in both Houses of Parliament to enable the instrument to be brought into effect) This would ensure that data subject protection could not be watered down without parliamentary approval and only in accordance with the data protection principles, and notably in giving further effect to conditions 5(a-d) and 6 in Schedule 2 of the DPA 1998

The data protection privacy statement (mentioned in the PIU Report) is a metastatement, like the data protection principles or the ECHR Convention rights, and should be 'read into' policies, procedures and practices – rather than being tediously worked into everything, service by service, as envisaged presently by the Government It is, instead, something that public authorities should sign up to, after approval by the OIC of a public authority's data protection measures – say, after successful notification

An adjunct to this process, and a subsidiary recommendation, should be

5.2.2.1. A scheduling mechanism for information-sharing protocols

all of which should operate to an OIC-agreed format which would act as a template A similar standardisation could be applied to agreements on data protection with contractors and data processor organisations

OIC approval of these schedules, alongside the notification itself, would enable a public authority to get the data protection privacy statement seal of approval. OIC 'signing-off' of the privacy statement should be the means of validating compliance with the Public Services Trust Charter (itself a metastatement), the 'sign-off' leading to the awarding of the Charter 'mark' in relation to the data protection duty

5.2.3. Government proposals for training must ensure that managers understand information processes thoroughly.

To be effective, the management level of public authorities must grasp the vertically-integrated nature of information processes Without this knowledge, strategic management thinking will be insufficiently grounded in the realities of these processes This knowledge should help to ensure that strategic direction is satisfactorily linked to routine operations, and that feedback is also received from lower levels of the organisation Processes must join up vertically as well as horizontally

There is always a danger that high-level statements can be superficial in their grasp of the significance of parts of processes at lower levels of responsibility in terms of the whole People need to be encouraged to think 'outside of the box'. The categories of thought that tend to shape government initiatives – and which tend to be couched in 'mission statementese' – need to be challenged. There is the risk that the tendency to central control and specification will stifle the necessary degree of initiative which leads to real internalisation of values

All of the above-mentioned changes, desirable in themselves, will only get us so far The ontological void, having been scaled at the edges, needs to be filled We have examined at length the shortcomings of a rights-based approach. A Public Services Trust Charter is simply more of the same – more well-meaning paper. We need words that can be translated into effective actions to ensure that *duties* are kept As O'Neill [18] has put it so succinctly

> Rights are not taken seriously unless the duties that underpin them are also taken seriously, these duties are not taken seriously unless there are effective and committed people and institutions that can do what they require

Trust is not going to come about by bureaucratic *fiat*. It cannot be claimed like a right Trust will be conferred (as with respect), being ontologically prior to a right, when something is seen as being worthy of trust, worthy of allegiance We therefore come on to those broader issues raised at the beginning of the recommendations

5.2.4. The public interest test needs to be modified by a change of emphasis.

Improvement here begins with the more logical approach suggested for any future Information Act The continuum of information concept suggests that the first question should be whether any request for information (personal or otherwise within a unified test of the kind indicated earlier) involves third parties and their personal information Such a test would then work to confidential information (which was not necessarily personal), until it came to information which could be divulged straightforwardly.

This changes the balance in favour of protecting privacy from the current bias in FoIA, but it does so in a structured way which builds on the data protection principles and confidentiality. The test is not simply reducible to the consequentialism of avoiding actions in breach of confidence This is because the test concerned as a unified process between data protection and freedom of information is deontological, with its emphasis on duties – of public authorities, organisations, individuals – rather than on a teleological end of a right to information (without any duty on requestors not to abuse the right beyond not being obviously vexatious) Worse, such a right only exists as a hypothetical imperative; the duty to safeguard privacy can be derived from a categorical one A unified test would properly reflect the balance of interest between openness and closure, the proposed test for FoIA currently is unlikely to do so

Vociferous pressure groups are hypersensitive to the perceived threat of state bodies to personal (informational) privacy, and reflect a narrow sectional view (inevitably rights-based rather than duty-based) expressing a particular kind of libertarian sentiment That this view has eloquent advocates does not of itself guarantee its truth The empirical evidence from five decades of crime figures suggests that this approach to law has not guaranteed the majority of the population greater security or physical privacy Yet it is further modification of the law in the direction of a rights-based approach that is advocated both by FoIA and the PIU Report

5.2.5. The concept of reciprocity needs to be introduced into English jurisprudence.

The concept of *reciprocity* (the duty not to abuse rights, and to confer them on others) needs to be realised in law as *proportionality* has already been Reciprocity will enable the law to go beyond the mere balancing of rights. Effectively, anyone claiming a right in court – Article 8, say – would have their duty not to abuse the right taken into account For example, a person claiming the Article 8 right to a private and family life in relation to housing, against a housing authority seeking eviction would have actions such as non-payment of rent or anti-social behaviour counted against them in terms of a general duty not to abuse the right The point is that such behaviour needs to be seen in duty-breaking terms· that is the key It is interesting that the prohibition of the abuse of rights in Article 17 does not appear to have had much effect in human rights cases so far in preventing abuses which create public disquiet, justifying the need for a purposive concept like reciprocity to give legal force to this duty

In relation to freedom of information and its interaction with personal and confidential information, the principle makes the reason for asking for information relevant – the right to information is predicated on the basis of a duty not to use the information for malicious purposes Guarding against misuse is the reason why the public interest test and third party concerns make the policing of the boundary between disclosure and non-disclosure an intensional matter of belief, judgement, and purpose, not just an extensional one of avoiding actionable breaches of confidence

It is unlikely that this principle would be allowed to be admitted into the law simply via the margin of appreciation of European human rights law, it is deontological, rather than sharing in the current rights-based teleology, and shows the need for 'pragmatic purposiveness' But the central issue remains obligation needs to be placed at the heart of the individual's relation to others as a core concept of the law Without it, respect for others' privacy will be difficult to sustain against the seductively selfish claims of rights merely to one's own

5.2.6. Serious consideration should be given to creating a statutory tort of infringement of privacy.

This question brings us back to the issue with which we began, and which would form a substantial part of the practical filling of the ontological void already identified There have been torts relating to physical privacy for a long time.

- nuisance
- trespass
- trespass as to person

Nuisance – in relation to noise – has been augmented by the Environmental Protection Act 1990 A new tort – of harassment – emerged in *Burris v Azadani* [19] in 1995, and led, after a number of high-profile cases of stalking to the Protection from Harassment Act (PFHA) 1997 Harassment and molestation had been discussed some four years earlier in the *Infringement of Privacy* consultation document [20], but trespass (including to person) is different from nuisance, which is different from harassment To subsume these all under one heading would obscure some important features between these different tortious aspects of privacy

Since the opportunity afforded by the *Infringement of Privacy* paper was not taken in the early 1990s, other activity has taken place This has happened because of the effects on English common law of the requirement in the HRA 1998 for courts 'to give effect to' the convention rights We have already related the emergence of a right to privacy in the *Douglas* case [21] acknowledged by Sedley LJ, arising out of Article 8, ECHR, which relates to privacy *per se*, physical and informational This right, as realised in DPA 1998, is essentially one claimed against organisations, including public authorities Its effects against individuals – such as enforcing protection against third parties – are horizontal ones, obtained via a claim against a breach of duty by an organisation or legal person

The arrival of PFHA 1997 represents the acceptance of specific statutory torts relating to privacy between individuals A Privacy Act for infringement of privacy by individuals against individuals would close the gap in the range of tortious remedies It would also provide the legal muscle to articulate the bones of the right to quiet enjoyment existing both in common law and in Article 1, Protocol 1 of the ECHR,

and take us beyond the 'judge-made' law of interpreting the HRA 1998 into common law, however well-intentioned

Reciprocity suggests that the duty to confer this on others by both legal and natural persons is the (ontologically) prior requirement The duty not to abuse rights would also imply that a claim of infringement of privacy could not be a defence against a legitimate investigation into criminal behaviour, or the exposure of hypocritical actions by powerful public figures

Accepting the statutory tort of infringement of privacy, embodying it in a Privacy Act, and accommodating the ramified definition of privacy into our jurisprudence, along with reciprocity, takes us much closer to the culture of privacy with the private autonomous data subject at its heart The checks on the infringement of privacy must nonetheless be subject to balances – there must be sufficient purchase upon criminality and terrorism to ensure that privacy can actually be delivered for the majority of citizens

This balance of higher-order duties and rights must be made and remade through plural politics The existence of private space is an essential feature of a plural society, and a culture of privacy its civil expression

5.2.7. There needs to be a programme of education in civic values and for the development of character.

To secure the health of a civil society valuing privacy, there needs to be such a programme which would begin the lasting changes to the broader political culture, inculcating the ideas of duty to, and respect for, others, notably for their private lives and quiet enjoyment, and promoting the ideal of the private autonomous citizen This would not merely be a matter of formal education in schools, but would involve promoting these ideas to the general public, setting out the basic civil obligations of every citizen

Such a programme would also involve a change of emphasis in educational thinking away from the instrumentalism of meeting targets and improving examination league

table performance there would be a requirement to develop 'rounded' citizens An education placing value on more than simply academic or vocational success might also be more attractive to students fatigued by utilitarian considerations Education needs to foster the development of character; there needs to be a recognition of the need for being a good citizen, rather than merely a clever one The future of our civil society rests upon the development of mature autonomous adults.

NOTES

CHAPTER 1 INTRODUCTION

1 Sexual Offences Act 1967 (1967 c 60).

2 Mill, JS· *On Liberty* (1859), ed Himmelfarb, Penguin, 1974 [1985]

3 Kant, Immanuel *The Metaphysics of Morals* [1797], trans and ed Gregor, M, Cambridge, 1996, in 'The Doctrine of Right', at 6 224

4 Privacy Act, 5 USC 552a, 1974

5 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [ETS no. 108] 28 January 1981 (entered into force 1 October 1985) [Council of Europe Convention 1981 on data protection]

6 Report of the Committee of Privacy (Cmnd. 5012, July 1972)

7 Data Protection Act 1984 (1984 c 25)

8 Document 395L0046 95/46/EC Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Official Journal L281, 23/11/1995, p0031-0050)

9 Data Protection Act 1998 (1998 c 29)

10 Human Rights Act 1998 (1998 c 42).

11 In the Paul Sieghart Memorial Lecture, 'Activism and Restraint Human Rights and the Interpretative Process', 20 April 1999, London

12 Rawls, John, *A Theory of Justice*, Oxford, 1970 [1973]

13 Nozick, Robert *Anarchy, State and Utopia*, Basic Books, 1974

14 Described in Graham, D, and Clarke, P *The New Enlightenment*, Macmillan, London, 1986

15 In Paul, et al , *Property Rights*, Cambridge, 1994

16 Nagel, Thomas, *Equality and Partiality*, Oxford, 1991

17 Paul, et al , op cit

18 Scruton, Roger, *The Meaning of Conservatism*, Penguin, 1979
Also Locke, John, *Two Treatises of Government*, ed Laslett, Cambridge

19 The National Council for Civil Liberties (NCCL) was founded in 1934 by the journalist Ronald Kidd to protect and promote civil liberties and human rights NCCL was relaunched as Liberty on 24 January 1989, coinciding with the three hundredth anniversary of the 1689 Parliamentary Convention leading to the

British Bill of Rights At the time of writing, the Director of Liberty is John Wadham.

20 In *Infringement of Privacy*, Lord Chancellor's Dept Consultation Paper 1993

21 Berlin, Isaiah, 'Two Concepts of Liberty' (1958) in *The Proper Study of Mankind,* ed Hardy and Hausheer, Pimlico, 1998

22 Rawls, op cit

23 Nagel, op cit

24 Klug, Francesca, *Values for a Godless Age*, Penguin, 2000

CHAPTER 2 PRIVACY

1 In *Infringement of Privacy*, Lord Chancellor's Dept Consultation Paper 1993

2 In Paul, et al *Property Rights*, Cambridge, 1994, pp241n

3 Reference to *Two Treatises of Government*, Second Treatise, s27, ed Laslett, Cambridge, quoted in Ryan, op cit

4 Ryan, op cit

5 Ryan, op cit

6 In Paul, et al ibid, pp259n

7 Munzer, op cit

8 In *Utilitarianism,* Cambridge, 1973

9 Paul Sieghart Memorial Lecture, 'Activism and Restraint. Human Rights and the Interpretative Process', 20 April 1999, London

10 Scruton, Roger, *The Meaning of Conservatism*, Penguin, 1979, pp16-17

11 Quoted from Alexis de Tocqueville, *Democracy in America* (Vol I, ch xv), by Himmelfarb in the footnote to p62, in Mill, JS, *On Liberty* (1859), ed Himmelfarb, Penguin, 1974 [1985], in comparison with Mill's use of 'tyranny of the majority' pp62-63

12 In the 1998 National Heritage Lecture 'Constitutional Change in the United Kingdom British Solutions to Universal Problems', US Supreme Court, 11 May 1998

13 Porter, Roy, *English Society in the Eighteenth Century*, Penguin

14 Porter, op cit Ch 7

15 Report of the Committee on Homosexual Offences and Prostitution (Cmnd 247. 1957) [The Wolfenden Report]

16 Wolfenden Report, op cit, para 62.

17 Mill, JS *On Liberty,* ed Himmelfarb, op cit ,, pp119-120, the argument acknowledged at the time by HLA Hart and Lord Devlin, see Dworkin, R, ed *The Philosophy of Law*, 1977 (1982), Oxford

18 Rosen, Allen D *Kant's Theory of Justice,* Cornell, 1993 (1996), reference to Kant's argument in the Doctrine of Right, in *The Metaphysics of Morals* [1797] trans and ed Gregor, M, Cambridge, 1996

19 In *Infringement of Privacy,* op cit.

20 ibid

21 ibid re Report of the Committee of Privacy (Cmnd 5012, July 1972)

22 ibid re Report, (Cmnd 7341, 1978).

23 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [ETS no 108] 28 January 1981 (entered into force 1 October 1985) [Council of Europe Convention 1981 on data protection]

24 In *Infringement of Privacy*, op. cit , re Report, (Cm 1102, June 1990)

25 ibid. re Review of Press Self-Regulation (Cm 2135, January 1993)

26 *Infringement of Privacy*, op cit

27 Korff, Douwe, *Study on the protection of the rights and interests of legal persons with regard to the processing of personal data relating to such persons*, Commission of the European Communities (Study Contract ETD/97/B5-9500/78)

28. Council of Europe Convention 1981, op cit

29 *Local Government Chronicle*, 20 October 2000, re *County Properties Ltd v The Scottish Ministers* [2000] SLT 546 (Outer House), 16 August 2001 (Inner House)

30 Berlin, Isaiah, 'Two Concepts of Liberty' (1958) in *The Proper Study of Mankind*, ed H Hardy and R Hausheer, Pimlico, 1998

31 Berlin, op cit p197

32 Berlin, op cit p216

33 Berlin, op cit p228

34. Berlin, op cit. p241

35 Berlin, op cit p242

36 *Human Rights Act An Introduction*, HRG1 10/2000. p9

37 Rawls, John, *A Theory of Justice*, Oxford 1971[1973]

38 Rawls, op cit p554

39. Rawls, op cit p560

40 Nagel, Thomas, *Equality & Partiality*, Oxford, 1991

41 Nagel, op cit pp15-16

42 Nagel, op cit p17

43 Nagel, op cit p19

44 Nagel, op cit. p32

45 Eliot, TS, 'Choruses from 'The Rock'' in *Collected Poems 1909-1962*, Faber & Faber 1974 [1983], Part VI, line 23 (p174)

46 Nagel, op cit p40

47 Hare, RM, *Freedom and Reason*, Oxford, 1963

48 Nagel, op cit p46

49 Nagel, op cit p52

50 Nagel, op cit p83

51 Nagel, op cit. p156

52 Nagel, op cit p156

53 Hare, op cit

54 Nagel, op cit p162

55 Nagel, op cit. p164

56 Nagel, op cit. p165

57 Klug, Francesca, *Values for a Godless Age*, Penguin, 2000.

58 Document 395L0046 95/46/EC Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Official Journal L281, 23/11/1995, p0031-0050)

59 Klug, op cit

60 Klug, op cit p32

61 *Council of Civil Service Unions v Minister for the Civil Service* [1985] AC 375 (the GCHQ case)

62 *Associated Picture Houses v Wednesbury Corporation* [1948] 1 KB 223

63 *Associated Picture Houses v Wednesbury Corporation* ibid.

64 Klug, op cit p39

65 The GCHQ case, quoted in Wadham & Mountfield, *Human Rights Act 1998*, Blackstone, 2nd ed 2000

66 Wadham & Mountfield, op cit p19.

67 Clements, Luke; Research Fellow, Cardiff Law School, University of Wales, view expressed at Human Rights Act one-day course, London 28 March 2001, and in course material

68 *Regina v DPP, ex parte Kebilene* [1999] 3 WLR 972, in Wadham & Mountfield q v

69 *Douglas and others v Hello! Ltd* [2001] EMLR 199

70 Quoted in ACTNOW, May 2001, a data protection local government newsletter

71 Korff, op cit, pp31n

72 Klug, Francesca, speech at LSE, London, 17 May 2001. "Human Rights Cause of or cure for the 'moral crisis' in liberal democracies?"

CHAPTER 3 COMPLIANCE

1 Carey, Peter *Blackstone's Guide to the Data Protection Act 1998*, Blackstone Press Ltd. 1998, pp52n

2 ibid p53.

3 ibid p53.

4 Birkinshaw, Patrick *Freedom of Information,* Butterworths, 2001 (3rd ed), pp346-347.

5 ibid p351

6. ibid p352

7 Home Office, ch5 of the Guidance on Statutory Crime & Disorder Partnerships – Information Exchange

8 Davies, JE, and Oppenheim, C *Study on the Availability and Use of Personal Information in Public Registers* (Final Report to the Office of the Data Protection Registrar), Loughborough University, Dept of Information Science, September 1999

9 ibid p15.

10 *The Times*, Saturday 17 November 2001, p10 "Sales of voters' list a breach of privacy"

11 Davies & Oppenheim, op cit. p18

12 Representation of the People Act 2000.

13 Davies & Oppenheim, op cit pp22n.

14 ibid p29

15 Quoted in ACTNOW, May 2001, op cit cf Chapter 2, PRIVACY, 58 above

16 Birkinshaw, op cit p51

17 SI 2000 No 2699 The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

18 Birkinshaw, op cit p55

19 *Computer Weekly*, 24 August 2000 "UK. the e-commerce pariah?"

20 Brown, David *Cybertrends,* Viking, 1997, pp18n

21 ibid. p36

22 ibid p120, re Tim May.

23 ibid p194

24 *Computer Weekly*, op cit "'We listened to industry on RIP Act' says Straw".

25 ibid

26 Gauthronet, S, and Nathan, F, (ARETE Computer co-operative) "On-line services and data protection and the protection of privacy" (Study for the Commission of the European Community (DG XV).), 1998

27 ibid p127.

28 OIC DPA 1998 Compliance Advice. Secondary Use of Personal Data Held for the Collection and Administration of the Council Tax (26/6/01)

29 Hasan, Ibrahim, in *IRRV Insight Magazine* July 2000 "Legal Update No Chinese walls!", pp14-15.

30 ibid , Lord Templeman in *Hazell v Hammersmith & Fulham*, 1992, quoted by Hasan

31 OIC DPA 1998 Compliance Advice, cf 28 above

32 ibid

33 Home Office Guidance, cf. 7 above

34 ibid

35 OIC· DPA 1998 Compliance Advice· Subject Access Rights & Third Party Information (02/03/00, version 2)

36 ACTNOW Circular May 2001, cf 15 above

37 OIC DPA 1998 Compliance Advice, cf. 15 above

38 *Gaskin v United Kingdom* [1989] 12 EHRR 36

39 OIC CCTV Code of Practice, July 2000

40 *The Times* Law Reports 18 December 1997, (QB Div)

41 Cabinet Office website, news release CAB 314/00 28 September 2000, and background paper, see Chapter 4, DISCUSSION, 10

42 House of Commons Home Affairs 2nd Report, re Q217. (Web version prepared 28 March 2001, published report ordered to be printed by the House of Commons 20 March 2001)

43 BBC News Online UK· Thursday 13 July 2000, "No more benefit – you're dead", see also *The Observer* 18 February 2001; Lambeth Council sought to get rid of Capita see *This is London* 29 June 2001

44. Europol Convention, 26 July 1995, coming into force on 1 October 1998

45 Anti-terrorism, Crime & Security Bill, House of Lords version, 10 December 2001

46 Anti-terrorism, etc Bill, Part 11, s102(6)(b), Act, Part 11, s102(3)(b)

47. Anti-terrorism, etc Bill, Part 3, s17(3), Act – omitted, see Government amendment, Bill, s17(5) and Act, s17(5)
48. House of Commons Hansard, 12 December 2001, col 902-903
49 House of Commons Hansard, 13 December 2001, col. 1111
50 House of Lords Hansard, 13 December 2001, col 1421.
51. ibid col 1422-1423
52. ibid col 1431

1 Nagel, Thomas, see Chapter 2, PRIVACY, 28, et seq

2 Rawls, John; see Chapter 2, PRIVACY, 25, et seq

3 Klug, Francesca, see Chapter 2, PRIVACY, 45, et seq.

4 Kant, Immanuel, *Groundwork of the Metaphysics of Morals* (1785), Section 1, 4 393 (trans Gregor, M; Cambridge, 1998.)

5 *Campbell v MGN Ltd* , (27 March 2002) Morland J, QB Div. In *Times Law Reports*, 29 March 2002.

6 *Campbell v MGN plc* (14 October 2002) CA· Lord Phillips of Worth Matravers MR, Chadwick and Keene LJJ On ICLR website (www lawreports co uk)

7 Lasch, Christopher, *The Revolt of the Elites and the Betrayal of Democracy*, Norton, (1995), p85

8 Wadham, John, et al , *Blackstone's Guide to the Freedom of Information Act 2000*, Blackstone Press Ltd , (2000), p57

9 *Regina v City of Wakefield Metropolitan Council & another ex parte Robertson* (16 November 2001) Kay J

10 Cornford, T, The Freedom of Information Act 2000 genuine or sham? *Web Journal of Current Legal Issues* [online], 2001 (3)

11 *'Privacy and data-sharing The way forward for public services'* A Performance and Innovation Unit Report, April 2002 The Cabinet Office

12 ibid. Section 3 and p5 of the Executive Summary.

13 ibid point 3 61.

14 ibid point 4 02

15 ibid point 4 03

16 ibid point 5 04.

17 ibid Box 6 2

18. ibid point 6 29

19 ibid point 7 11

20 ibid, point 8 31

21 ibid point 9 16

22 Raab, CD, 'Privacy in the public interest' *The Guardian*, Saturday, September 21, 2002 Also Raab, CD, 'Electronic Service Delivery in the UK· Pro-action and privacy protection ' In Prins JEJ (ed) *Designing e-Government on the crossroads*

of technological innovation and institutional change Kluwer Law International, 2001

23. Raab, CJ, and Bennett, CJ, 'Taking the measure of privacy can data protection be evaluated?' *International Review of Administrative Sciences*, 1996, 62 (4), p541 Also Raab CD, 'From Balancing to Steering New Directions for Data Protection' In Bennett, CJ, and Grant, R (eds). *Visions of Privacy*, University of Toronto Press, 1999 p83, and Raab, 2001, op. cit
24. Raab, CD, 'Co-producing data protection', *International Review of Law Computers and Technology*, 1997, 11(1), p17. Also Raab, 1999, p83, op cit
25. Raab, 1996, p 551, op cit
26 Raab, 1996, ibid
27. Rule, JB, *Private Lives and Public Surveillance*, Allen Lane, London, 1973, ch 9
28 Rule, JB, *et al* , *The politics of privacy*, Elsevier, New York, 1980, ch 18, p152
29. Rule, JB, *et al* 1980, ch 22, p187, op cit

CHAPTER 5 CONCLUSIONS

1 In *Utilitarianism*, Cambridge, 1973 See Chapter 2, PRIVACY, 8

2 Hume, David, *A Treatise of Human Nature* (1739-40), Book II, 2nd Ed (Ed Selby-Bigge, LA, revised by Nidditch, PH) Oxford 1978 (1981). p415:
"Reason is, and ought only to be the slave of the passions, and can never pretend to any other office than to serve and obey them "

3 Cornford, T, The Freedom of Information Act 2000 genuine or sham? *Web Journal of Current Legal Issues* [online], 2001 (3) See Chapter 4, DISCUSSION, 10.

4 *Infringement of Privacy* Lord Chancellor's Department Consultation Paper, July 1993 see Chapter 2, PRIVACY, 1.

5 *Associated Picture Houses v Wednesbury Corporation* [1948] 1 KB 223 See Chapter 2, PRIVACY, 62,63

6 Lord Denning, MR *The Discipline of Law*, Butterworths, London, 1979

7 Denning, op, cit p12

8. Denning, op cit p13

9 Denning, op cit p17, quoting Viscount Dilhorne HL, in *Stock v Frank Jones (Tipton) Ltd* [1978] 1 WLR 231.

10 Denning, ibid

11 Denning, op cit p21

12 Rosen, Allen D *Kant's Theory of Justice*, Cornell University Press, 1993 [1996], pp105-111

13 Bainbridge, D, and Pearce, G 'Tilting at windmills – has the new Data Protection law failed to make a significant contribution to rights of privacy?' *The Journal of Information, Law and Technology* [online], 2000 (2). (URL http //elj warwick ac uk/jilt/00-2/bainbridge html) [Accessed 22 May 2003]

14 'Tax records 'for sale' scandal', BBC News Business, Thursday 16 January 2003, at http //news bbc co uk/1/hi/business/2662491 stm.

15 *'Privacy and data-sharing The way forward for public services'* A Performance & Innovation Unit Report, April 2002 The Cabinet Office. see Chapter 4, DISCUSSION, 10

16 Rule, JB, *et al* , *The politics of privacy*, Elsevier, New York, 1980, ch 18, p152 See Chapter 4, DISCUSSION, 28

17. *'Privacy and data-sharing The way forward for public services'* op cit.

18 O'Neill, Onora, *A Question of Trust* (BBC Reith Lectures 2002), Cambridge, 2002, p30

19 *Burris v Azadani* [1995] 4 ALL ER 802, Court of Appeal on 27 July 1995

20 *Infringement of Privacy* op cit.

21 *Douglas and others v Hello! Ltd* [2001] EMLR 199 see Chapter 2, PRIVACY, 57

BIBLIOGRAPHY

List of United Kingdom Statutes

Access to Personal Files Act 1987 (1987 c 37).

Anti-terrorism, Crime and Security Act 2001 (2001 c 24)

Companies Act 1985 (1985 c 6).

Computer Misuse Act 1990 (1990 c 18)

Crime and Disorder Act 1998 (1998 c 37)

Criminal Law Amendment Act 1885 (48 & 49 Vict c 69)

Data Protection Act 1984 (1984 c 25)

Data Protection Act 1998 (1998 c 29)

Electronic Communication Act 2000 (2000 c.7).

Environmental Protection Act 1990 (1990 c 43)

Freedom of Information Act 2000 (2000 c 36)

Human Rights Act 1998 (1998 c 42)

Interception of Communications Act 1985 (1985 c 56)

Local Government Act 1972 (1972 c 70)

Local Government Act 2000 (2000 c 22)

Local Government Finance Act 1992 (1992 c 14)

Protection from Harassment Act 1997 (1997 c 40)

Public Interest Disclosure Act 1998 (1998 c 23)

Public Records Act 1958 (6 & 7 Eliz 2 c 51)

Regulation of Investigatory Powers Act 2000 (2000 c 23)

Representation of the People Act 2000 (2000 c 2)

Sexual Offences Act 1967 (1967 c 60)

Terrorism Act 2000 (2000 c 11)

United Kingdom Statutory Instruments

SI 2000 No 2699 The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

List of Cases

Associated Picture Houses v Wednesbury Corporation [1948] 1 KB 223

Burris v Azadani [1995] 4 ALL ER 802, Court of Appeal on 27 July 1995

Campbell v MGN Ltd , (27 March 2002) Morland J, QB Div In *Times Law Reports*, 29 March 2002

Campbell v MGN plc (14 October 2002) CA: Lord Phillips of Worth Matravers MR, Chadwick and Keene LJJ On ICLR website (www lawreports co.uk).

Council of Civil Service Unions v Minister for the Civil Service [1985] AC 375.

County Properties Ltd v The Scottish Ministers [2000] SLT 546 (Outer House), 16 August 2001 (Inner House)

Douglas and others v Hello! Ltd [2001] EMLR 199

Gaskin v United Kingdom [1989] 12 EHRR 36

Hazell v Hammersmith & Fulham London Borough Council [1991] HL, ([1992] 2 AC 1)

Regina v Brentwood Borough Council ex parte Peck [1997] *The Times* Law Reports 18 December 1997 (QB Division)

Regina v City of Wakefield Metropolitan Council & another ex parte Robertson (16 November 2001) Kay J

Regina v DPP, ex parte Kebilene [1999] 3 WLR 972

Stock v Frank Jones (Tipton) Ltd [1978] 1 WLR 231.

Background

Acton, HB *Kant's Moral Philosophy*, Macmillan, 1970 [1979]

Crook, A 'Data protection in the United Kingdom, part 2', *Journal of Information Science*, 1983, 7 (2), pp47-57

David, R, and Brierley, JEC *Major Legal Systems in the World Today*, Stevens, 1985 (3rd English ed.)

Jowell, J and Cooper, J (eds)· *Understanding Human Rights Principles* (JUSTICE Series) Hart Publishing, 2001

Kosten, F and Pounder, C. 'The EC Data Protection Directive 1995 An analysis', Web Journal of Current Legal Issues [online], 1996, 2 (URL http·//webjcli ncl ac uk/1996/issue2/kosten2 html) [Accessed 12 May 2003]

Lacey, AR· *Robert Nozick*, Acumen, 2001

Kant, Immanuel· *Critique of Practical Reason* (1788), ed Gregor, Cambridge, 1997

Makkan, Sam. *The Human Rights Act 1998 The Essentials*, Callow Publishing, London, 2000

References

ACTNOW Circular May 2001 At ACTNOW website (http //www actnow org uk) Data protection newsletter for the public sector. [Accessed June 2001]

BBC News Online UK. Thursday 13 July 2000, "No more benefit – you're dead", (see also *The Observer* 18 February 2001, Lambeth Council sought to get rid of Capita see *This is London* 29 June 2001) (URL. http //news bbc co uk/low/english/uk/newsid_831000/831911 stm) [Accessed 11 December 2001]

BBC News Online UK Business, Thursday 16 January 2003, 'Tax records 'for sale' scandal' (URL http //news bbc.co uk/1/hi/business/2662491.stm) [Accessed 16 January 2003]

Bainbridge, D, and Pearce, G 'Tilting at windmills – has the new Data Protection law failed to make a significant contribution to rights of privacy?' *The Journal of Information, Law and Technology* [online], 2000 (2) (URL. http //elj warwick ac uk/jilt/00-2/bainbridge html) [Accessed 22 May 2003]

Berlin, Isaiah· 'Two Concepts of Liberty' (1958) in *The Proper Study of Mankind*, ed Hardy and Hausheer, Pimlico, 1998

Birkinshaw, Patrick *Freedom of Information,* Butterworths, 2001 (3rd ed)

Brown, David *Cybertrends,* Viking, 1997.

Carey, Peter: *Blackstone's Guide to the Data Protection Act 1998*, Blackstone Press Ltd 1998

Computer Weekly, 24 August 2000· "UK the e-commerce pariah?" Reed Business Information

Computer Weekly, op cit "'We listened to industry on RIP Act' says Straw". Reed Business Information

Cornford, T 'The Freedom of Information Act 2000 genuine or sham?' *Web Journal of Current Legal Issues* [online], 2001 (3) (URL· http //webjcli ncl ac uk/2001/issue3/cornford3 html) [Accessed 02 June 2003]

Davies, JE, and Oppenheim, C *Study on the Availability and Use of Personal Information in Public Registers* (Final Report to the Office of the Data Protection Registrar), Loughborough University, Dept of Information Science, September 1999

Denning, Rt Hon Lord, MR *The Discipline of Law*, Butterworths, London, 1979

Dobson, Nicholas 'Not just anybody', *Local Government Chronicle*, 20 October 2000, p14 EMAP Public Sector Management

Eliot, TS 'Choruses from 'The Rock'' in *Collected Poems 1909-1962*, Faber & Faber 1974 [1983], Part VI, line 23 (p174).

European Union Europol Convention, 26 July 1995, coming into force on 1 October 1998 (Official Journal C 316, 27/11/1995)

European Union Document 395L0046 95/46/EC Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Official Journal L281, 23/11/1995, p0031-0050)

Gauthronet, S, and Nathan, F, (ARETE Computer co-operative). "On-line services and data protection and the protection of privacy" (Study for the Commission of the European Community (DG XV)), 1998

Ghandi, PR: *International Human Rights Documents*, 1st ed , Blackstone Press Ltd , 1995 (Contains text of European Convention on Human Rights).

Graham, D, and Clarke, P *The New Enlightenment*, Macmillan, London, 1986

Hare, RM *Freedom and Reason*, Oxford, 1963

Hasan, Ibrahim "Legal Update: No Chinese walls!" in *IRRV Insight Magazine* July 2000

Hume, David, *A Treatise of Human Nature* (1739-40), Book II, 2nd Ed (Ed Selby-Bigge, LA, revised by Nidditch, PH) Oxford 1978 (1981)

Irvine of Lairg, Lord 1998 National Heritage Lecture 'Constitutional Change in the United Kingdom: British Solutions to Universal Problems', US Supreme Court, 11 May 1998 (URL http //www open gov uk/lcd/humanrights/speeches/11-5-98 htm) [Accessed 22 November 2000].

Irvine of Lairg, Lord Paul Sieghart Memorial Lecture, 'Activism and Restraint Human Rights and the Interpretative Process', 20 April 1999, London (URL http://www open gov uk/lcd/humanrights/speeches/20-4-99 htm) [Accessed 20 December 2000]

Kant, Immanuel· *Groundwork of the Metaphysics of Morals* (1785), trans Gregor, M, Cambridge, 1998

Kant, Immanuel *The Metaphysics of Morals* (1797), trans and ed Gregor, M, Cambridge, 1996

Klug, Francesca· *Values for a Godless Age*, Penguin, 2000

Klug, Francesca. Centre for the Study of Human Rights, London School of Economics, London, speech, 17 May 2001: "Human Rights· Cause of or cure for the 'moral crisis' in liberal democracies?". Home Office Human Rights Unit [Accessed 29 June 2001]

Korff, Douwe, *Study on the protection of the rights and interests of legal persons with regard to the processing of personal data relating to such persons*, Commission of the European Communities (Study Contract ETD/97/B5-9500/78).

Lasch, Christopher *The Revolt of the Elites and the Betrayal of Democracy*, Norton, 1995

Locke, John *Two Treatises of Government*, ed. Laslett, P, Cambridge, 1960 [1988]

Mill, JS *On Liberty* (1859), ed Himmelfarb, Penguin, 1974 [1985]

Nagel, Thomas *Equality and Partiality*, Oxford, 1991.

Nozick, Robert *Anarchy, State and Utopia*, Basic Books, 1974

O'Neill, Onora *A Question of Trust* (BBC Reith Lectures 2002), Cambridge, 2002

Paul, et al (eds) *Property Rights*, Cambridge, 1994

Porter, Roy: *English Society in the Eighteenth Century*, Penguin, 1982

Raab, CD 'Co-producing data protection', *International Review of Law Computers and Technology*, 1997, 11 (1), pp11-24

Raab, CD 'From Balancing to Steering: New Directions for Data Protection', in Bennett, CJ, and Grant, R (eds) *Visions of Privacy*, University of Toronto Press, 1999, pp68-93

Raab, CD: 'Electronic Service Delivery in the UK Pro-action and privacy protection' in Prins, JEJ (ed): *Designing e-Government on the crossroads of technological innovation and institutional change*, Kluwer Law International, Boston and The Hague, 2001

Raab, CD 'Privacy in the public interest', The Guardian, Saturday, September 21, 2002. (URL: http //www guardian co uk/bigbrother/privacy/blackmarket/story/0,12380,794283,00 html) [Accessed 30 May 2003].

Raab, CD, and Bennett, CJ 'Taking the measure of privacy can data protection be evaluated?' *International Review of Administrative Sciences*, 1996, 62 (4), pp535-556

Rawls, John *A Theory of Justice*, Oxford, 1970 [1973]

Rosen, Allen D: *Kant's Theory of Justice*, Cornell University Press, 1993 [1996]

Rule, JB. Private Lives and Public Surveillance, Allen Lane, London, 1973

Rule, JB, *et al* *The Politics of Privacy* Elsevier, New York, 1980

Scruton, Roger *The Meaning of Conservatism*, Penguin, 1979

Smart, JJC, & Williams, Bernard *Utilitarianism*, Cambridge, 1973

The Times, Saturday 17 November 2001, p10. "Sales of voters' list a breach of privacy"

United Kingdom Cabinet Office. *'Privacy and data-sharing The way forward for public services'* Performance and Innovation Unit Report, London, April 2002 (Ref CAB1 JO1-9063/0402/D16)

United Kingdom House of Commons. Home Affairs Committee Third Report. *Criminal Records* HC 285 of Session 1989-90 Chairman Sir John Wheeler HMSO, London

United Kingdom Home Office *Human Rights Act An Introduction*, HRG1 10/2000 Home Office Communications Directorate London

United Kingdom Home Office *Report of the Committee on Homosexual Offences and Prostitution* Chairman Sir John Wolfenden (Cmnd 247, 1957) HMSO, London

United Kingdom Home Office *Report of the Committee on Privacy* Chairman Kenneth Younger (Cmnd 5012, July 1972) HMSO, London

United Kingdom Home Office *Report of the Committee on Data Protection.* Chairman Sir Norman Lindop (Cmnd. 7341, 1978). HMSO, London

United Kingdom Home Office Report of the Committee on Privacy and related matters Chairman David Calcutt (Cm 1102, June 1990). HMSO, London

United Kingdom Home Office Guidance on Statutory Crime & Disorder Partnerships – Information Exchange
(URL http //www homeoffice gov uk/cdact/actgch5 htm) [Accessed 17 August 2001]

United Kingdom. Department of National Heritage *Report of the Review of Press Self-Regulation* Sir David Calcutt. (Cm 2135, January 1993) HMSO, London

United Kingdom Lord Chancellor's Department and Scottish Office *Infringement of Privacy* Consultation Paper 1993 (Ref. CHAN JO60915NJ 7/93) London

United Kingdom Office of the Information Commissioner DPA 1998 Compliance Advice. Subject Access Rights & Third Party Information (02/03/00, version 2) OIC, Wilmslow

United Kingdom Office of the Information Commissioner CCTV Code of Practice, July 2000 OIC, Wilmslow

United Kingdom Office of the Information Commissioner DPA 1998 Compliance Advice Secondary Use of Personal Data Held for the Collection and Administration of the Council Tax (26/6/01) OIC, Wilmslow.

United Kingdom House of Commons Home Affairs Committee Second Report Session 2000-01. *Criminal Records Bureau* Chairman Robin Corbett House of Commons Papers 227 TSO, London

United Kingdom House of Commons Hansard, 12 December 2001, col 902-903 TSO, London

United Kingdom House of Commons Hansard, 13 December 2001, col 1111 TSO, London

United Kingdom House of Lords Hansard, 13 December 2001, col 1421 TSO, London

United Kingdom. House of Lords Anti-terrorism, Crime and Security Bill HL Bill 33 10 December 2001. (via URL http://www parliament the-stationery-office co uk/pa/ld/ldbills htm for public bills, and downloaded as a pdf file)

United States of America. Privacy Act, 5 USC 552a, 1974

Wadham, J & Mountfield, H. *Blackstone's Guide to the Human Rights Act 1998*, Blackstone, 2nd ed 2000.

Wadham, John, et al , *Blackstone's Guide to the Freedom of Information Act 2000*, Blackstone Press Ltd , 2000