# Overlooked:

## Surveillance and personal privacy in modern Britain


**Gareth Crossman**

**with**

**Hilary Kitchin, Rekha Kuna**
**Michael Skrein and Jago Russell**



The Nuffield Foundation

LIBERTY
PROTECTING CIVIL LIBERTIES
PROMOTING HUMAN RIGHTS

# Overlooked:

## Surveillance and personal privacy in modern Britain

**Gareth Crossman**

**with**

**Hilary Kitchin, Rekha Kuna**
**Michael Skrein and Jago Russell**

LIBERTY

PROTECTING CIVIL LIBERTIES
PROMOTING HUMAN RIGHTS

## Acknowledgements

I would like to thank those who have offered advice and support during the course of this work. Particular mention is due to the project's academic mentor Professor Charles Raab whose many suggestions have proved invaluable and to Andrew Phillips who has supported this work throughout. Many others have offered their expertise and I would particularly like to thank Madeleine Colvin, Caspar Bowden, Jonathan Bamford, Simon Watkin, Phil Booth, Antony White QC, Alan Hawley and Colin Greene.

Thanks to the Nuffield Foundation for their sponsorship and funding of this work.

To former and present staff at Liberty to numerous to mention for their endless patience and to Sabina Frediani, Lee Rodwell and Jen Corlew for their editing abilities. My sincere thanks and gratitude go to Liberty's Director Shami Chakrabarti for her unflinching support and wise counsel throughout.

**Gareth Crossman**
**October 2007**

The Nuffield Foundation

*The Nuffield Foundation is a charitable trust established by Lord Nuffield. Its widest charitable object is 'the advancement of social well-being'. The Foundation has long had an interest in social welfare and has supported this project to stimulate public discussion and policy development. The views expressed are however those of the authors and not necessarily those of the Foundation.*

## Authors

**Gareth Crossman** is Liberty's Director of Policy.

**Hilary Kitchin** is a Policy Analyst with the Local Government Information Unit.

**Rekha Kuna** is an Associate Solicitor at Reed Smith Richards Butler LLP.

**Michael Skrein** is a Partner at Reed Smith Richards Butler LLP.

**Jago Russell** is Liberty's Policy Officer.

**Research assistance:** Kirsteen Shields, Dawn Sedman, Caoilfhionn Gallagher and Gaby Johnson.

# Overlooked:

## Surveillance and personal privacy in modern Britain

The last few years have been a difficult time for the protection of fundamental rights and freedoms in the United Kingdom. The misnamed and misjudged “War on Terror” alongside other authoritarian tendencies going even further back, have fostered a rather cavalier, almost “year nought” approach to long-held values in the oldest unbroken democracy on Earth. At a time, when some people seem ready to compromise over absolute rights such as the prohibition on torture and fair trial rights such as the right to be charged and tried before lengthy imprisonment, how much more vulnerable is the more qualified or balanced right to respect for our personal privacy? So at a time of “extraordinary rendition” and arbitrary punishment and detention, why should intrusions into personal privacy matter? Isn’t this a somewhat trivial concern in the greater scheme of things? The answer lies in the basis of democracy, rights protection and the essence of humanity itself.

As proponents of human rights, Liberty believes that every individual human life is so inherently precious, that it is to be treated with dignity and respect and subject to the values of equal treatment and fairness. The very moment that human beings form relationships, families and other associations, let alone complex modern societies, privacy becomes necessarily qualified. Without some proportionate and lawful intrusion, other vital concerns such as free speech, ministerial accountability, tax collection, child protection, let alone public safety would be impossible to pursue. Nonetheless, a society which does not pay sufficient regard to personal privacy is one where dignity, intimacy and trust are fatally undermined. What is family life without a little bit of personal space around the home? How do you protect people from degrading treatment (whether in hospital, prison or the home) without paying regard to their privacy? How are fair trials possible without confidential legal advice or free elections without secret ballots? Equally, whilst free speech, law enforcement and public health are often seen in tension with personal privacy, think of anonymous sources, vulnerable witnesses and terrified patients who may be more likely to seek help if their confidences are safe and perceived to be so.

Notwithstanding, the casual legislative attitude to privacy in recent years, the British public is rather more troubled. A YouGov poll commissioned by Liberty in September of 2007 showed 54 per cent of those questioned did not trust government and other public sector authorities to keep their personal information completely confidential. Forty-eight per cent think that these authorities hold too much of their personal information and 57 per cent think that "the UK has become a surveillance society".

One problem with privacy protection in this country is perhaps that too much has been left to the courts and not enough delivered by our politics. A two-sided litigation battle may be a good protection of last resort for the torture victim or the prisoner detained without law. Our courts have been strong and right in protecting individuals suffering the gravest violations of fundamental rights from policies based on overblown communitarian rhetoric. They have proved less effective in conducting the complex balancing acts necessary when personal privacy is at stake. When a young man appears in court complaining that his DNA is to be held indefinitely on a national database though he has never been charged, let alone convicted of a criminal offence, our courts have been too ready to see this as a matter of irritation rather than intrusion, when set against public interest arguments relating to crime detection. We would argue that the value of privacy is as much a societal interest as public protection. Behind the young man in this example sit thousands of others and an important aspect of the flavour of our democratic society itself. In a legal system essentially without "class actions", to view the argument as involving a light touch interference with one person versus sweeping societal benefit, is to miss the value of privacy and to set up a David and Goliath struggle with, in the absence of divine intervention, privacy and dignity as inevitable losers.

Gareth Crossman is the Policy Director of Liberty (the National Council for Civil Liberties), and one of the foremost experts on the law, ethics and practice of privacy protection in the United Kingdom. My outstanding colleague has completely transformed Liberty's policy reputation and influence in Westminster, Whitehall, and broader civil society. His background as a solicitor and journalist have produced an ethical brain which neither fears nor indulges the twin evils of legal and technological jargon that stand between so many people and proper debate about how best to protect their personal privacy. This work has been four years in the making. It is reasoned, reasonable and well-researched. Liberty and the Civil Liberties Trust are proud to present this as a powerful piece of advocacy of a democratic value that has been overlooked for too long.

**Shami Chakrabarti**
**Director of Liberty**
**October 2007**

# Contents

# Overlooked:

# Surveillance and personal privacy in modern Britain

## Executive Summary

The past decade has brought many threats to personal privacy. However, over the last two years in particular, growing nervousness in Westminster, the media and wider public opinion suggests that the time may be ripe for broad and balanced debate about this important democratic value.

The contrast between the final years of the 1990s and the start of the current decade is marked. The right to respect for privacy became enforceable in UK courts as recently as October 2000 via the Human Rights Act 1998. However the political context at the time gave privacy a difficult inception. The murder of Jamie Bulger in 1993, and the subsequent use of CCTV to help identify and convict his killers, struck a powerful chord with the public. Although there was little evidence that CCTV would actually deter crime, it became largely accepted with little debate over effectiveness or lack of regulation.

Within a year of the new privacy protections, the tragic events of September 11 2001 served further to entrench a belief that concerns over privacy were automatically trumped by the demands of national security. 'Nothing to hide, nothing to fear' became a well-worn mantra.

So what has changed? No single dramatic event has increased interest in privacy. Rather a series of factors have combined to swing the pendulum back towards this concern. The flagship ID card programme and other huge public IT projects have been regularly challenged over cost and efficacy. The media debate has developed so that privacy and crime-fighting imperatives are no longer seen as a simple trade-off. Further, the Information Commissioner's Office (ICO) has regularly voiced concerns over the lack of effective privacy protection and regulation.

Unfortunately, this late interest in privacy means that protection does not match the challenges of 2007. Data protection laws have become outdated and fail to keep pace with the reality of modern data processing; CCTV remains largely unregulated; expansion of the National DNA Database (NDNAD) has continued apace; targeted state surveillance has also grown and remains under regulated.

An overhaul of privacy protection is needed. This report makes a series of recommendations intended to improve the framework. This is not intended to champion privacy at the expense of crime detection, national security or other vital aim of the state. Rather it sets out to provide a proper regulatory regime, effective enforcement and improved accountability.

The report covers several forms of surveillance and their impact upon privacy. In particular the focus is on the Right to Respect for Privacy contained in Article 8 HRA and the framework of the Data Protection Act 1998 (DPA). The summary of findings and the most significant recommendations are as follows.

## Targeted Surveillance

This section considers the framework of state sanctioned surveillance against specific targets created under the Regulation of Investigatory Powers Act 2000. Surveillance takes place on a massive scale with nearly 440,000 authorisations for communications traffic data taking place between June 2005 and March 2006. The report concludes that although the basic structure is sound it lacks accountability and transparency. In particular, there is a need for judicial authorisation for the most intrusive forms of surveillance and an improved complaints mechanism. Further, the bar on intercepted material in criminal trials needs to be lifted.

## Mass Surveillance

The sheer growth and impact of mass databases has been a significant development over the last decade. Increasingly the boundary between mass and targeted surveillance is blurring due to the increased use of mass automated processes such as data mining and data matching. New data protection legislation is needed to allow better regulation of data and to improve the ability and resource of the ICO to provide effective enforcement. There should be greater accountability to parliament.

## Visual Surveillance

Daily exposure to mass CCTV surveillance is an all pervading reality of 2007. The UK is the world leader in CCTV use with approximately 4.2 million cameras in operation.

While CCTV has its uses, primarily in relation to crime detection, it remains relatively unevaluated in relation to crime prevention and cost effectiveness. The DPA fails to provide an effective enforcement tool. Compliance with more detailed guidance, such as that issued by the ICO, remains unenforceable and is largely dependant on proactive and responsible attitudes from individual local authorities and police authorities. New legislation is needed to effectively regulate CCTV.

## DNA

While there is a justification for the NDNAD, it is increasingly of concern. With an estimated 3.9 million samples, the NDNAD is five times larger than any other national database and contains samples taken from many who have never been convicted of any offence. This is largely due to successive acts of parliament rolling out the grounds for permanent retention to the current position where DNA can be taken and retained following arrest for any recordable offence. Expansion of the NDNAD by taking samples upon arrest rather than conviction has disproportionately affected black men with nearly 40% of black men represented, versus 13% of Asian men and 9% of white men. The effectiveness of mass roll out of the NDNAD is questionable, with no statistical evidence that expansion has improved crime-solving rates. This is largely explained by the fact that DNA is of relevance only to a small number of criminal offences, mainly those involving sexual assault or other

violence. There should be no further roll out of the grounds for retention. Samples should be deleted unless a person is convicted of a relevant offence or where there remains an ongoing investigation.

## Privacy and the Media

Developments in privacy law differ from other areas in this study. Rather than involving consideration of the legitimate limits of the relationship between the individual and the state developed through statute, it has tended to involve common law resolution between private parties. Privacy and the Media has also usually more directly involved consideration of potentially conflicting rights, typically setting Article 8 (the Right to Respect for Privacy and Family Life) Rights against Article 10 (the Right to Free Expression). The result has been a sometimes confusing array of competing caselaw.

# 1. Introduction

Writing about privacy presents a challenge. The subject matter is likely to change during the course of work, through the passing of new laws and interpretations made by courts. Disparate concepts of what 'privacy' is means that a single piece of work, conjoining state surveillance powers to media privacy to genetic privacy and so on is difficult.

At the start of this work it was predicted the report would recommend a single piece of privacy legislation. This would extend and enhance the right to privacy contained in Article 8 of the European Convention on Human Rights (ECHR). It would also address the shortfalls in protection offered by the Data Protection Act 1998 (DPA). As work progressed it became apparent that attempting to address such a range of issues in a single Act would make it cumbersome and unwieldy. Even if desirable, the prospects of such legislation reaching the statute book would be remote. There are also non legislative aspects of privacy protection, such as good practice, that are of great importance. Good practice on the use of CCTV or on press reporting have a preventative benefit preferable to legal sanction after the event.

The focus is primarily upon the public rather than private sector, this being Liberty's traditional area of concern. However, as is pointed out later in the work on surveillance, the relevance of the private sector is increasing particularly in relation to the holding and dissemination of mass data. Notwithstanding this there must be some limitation on the subject matter which is why private sector use of data, and other private sector issues such as workplace privacy, are not considered.

At the outset of the twenty-first century, it is clear that few public policy issues will attract more attention in the years ahead than the protection of privacy. Privacy is, to many concerned by ever increasing state powers of information retention and sharing, a right whose time has come. To others, privacy is seen as a hurdle preventing better law enforcement, counter-terrorism, public services and technological advancement.

Privacy's relatively recent arrival in the policy spotlight can be seen from the fact that those nations with written Constitutions and entrenched Bills of Rights have different forms of protection for privacy depending on when they were drafted. Older documents, such as the U.S. (1789), Irish (1937) and French (1958) Constitutions do not explicitly include a right to privacy, although their

courts have subsequently found privacy to be an 'unenumerated,' 'unspecified' or 'implicit' right. However, recently drafted Constitutions tend to include a specific right to privacy, often including detail on different aspects of the right[1].

Increased concerns about terrorism mean that privacy is getting much more attention internationally – but for the wrong reasons. New laws and political decisions internationally reflect a growing interest in new surveillance technologies that governments trust will enable them to prevent terrorist attacks or effectively fight crime.

In Britain, privacy's time in the spotlight will continue for the foreseeable future. Continued attention from the courts also appears likely, given the rapid development of case law relating to privacy over the short period since the Human Rights Act 1998 (HRA) came into force.

Media attention continues unabated as the courts continue to grapple with the competing demands of privacy and freedom of expression, and the question of whether there is a distinction between 'the public interest' and 'what interests the public'.

Future political attention to the issue of privacy is guaranteed by the fact that it is the Government's stated aim to use increased data-sharing and data-matching across public sector boundaries as part of its drive for 'joined-up government' and to 'modernise government'[2], but also by the fact that there is political awareness that such measures cannot be effective without public support[3]. Further, the Government has demonstrated through a range of statutory, regulatory and extra-parliamentary measures that it considers the value of privacy to be outweighed by a range of factors. Arguments put forward in favour of the Identity Cards Act 2006, surveillance and interception powers under the Regulation of Investigatory Powers Act 2000 and information sharing powers created by the Children Act 2004 all suggest that the right to privacy has not featured highly in the Government's reckoning.

However, privacy is increasingly an issue of national public interest. The national press carries stories about 'snoopers' and 'Big Brother' with increasing regularity. In November 2006 the Information Commissioner Richard Thomas introduced '*A Report on the Surveillance Society*'[4], specially commissioned for the 28th International Data Protection and Privacy Commissioners' Conference. Its first paragraph began with a statement of fact 'We live in a surveillance society. It is pointless to

---

[1] For example the South African Constitution, section 14 (1996), Constitution of the Republic of Hungary, Article 59 (1989).

[2] Performance and Innovation Unit Report (Lord Chancellor's Department) *Privacy and Data Sharing: The Way Forward for Public Services* (April 2002). The government's agenda in this regard does make provision for certain substantial privacy safeguards, but nevertheless there is cause for concern about possible legislation to allow sharing without consent.

[3] *ibid*., particularly 'Foreword by the Prime Minister', p. 4; Elizabeth France, former Information Commissioner, "The right to know," *The Guardian*, September 21st 2002 ("If government is seeking to gain our confidence it, more than others, must be ready to put in place the resources necessary to respond to our requests and to do so with a generous spirit where nuances of interpretation might allow argument aimed at restricting what might be released. To gain our confidence, crucial for the exploitation of new technology, government must set an example to others by demonstrating the importance of being open and accountable while respecting the right of each of us to private life.").

[4] *'A Report on the Surveillance Society' by Kirstie Ball, David Lyon, David Murakami Wood, Clive Norris and Charles Raab* – http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf

talk about surveillance society in the future tense'. In January 2007, perhaps in response to comments about ever increasing surveillance and data sharing, the former Prime Minister Tony Blair and others in government spoke of the need for greater information sharing between government departments[5]. Inherent was the implication that there were unhelpful barriers preventing information sharing taking place. As Schedules 2 and 3 to the Data Protection Act clearly state, the processing of data between government departments and between public bodies generally is permissible[6]. However it must also be processed for specified purposes, not be excessive and not kept longer than necessary. Then Prime Minister Tony Blair's intention might have been to argue for an extension of what was currently permissible. Unfortunately the examples he gave (information about those recently deceased and medical information following an accident) were situations where sharing would not be prevented. This does not help reasoned debate, as the reaction of anyone unaware of what is permissible would be that information sharing should of course be extended if it helps the recently bereaved or helps deal with a medical emergency.

## Different Aspects of Privacy

The simplest modern legal definition of privacy came from the 19th century American lawyer Judge Cooley, who defined it as "the right to be let alone"[7]. This is an essentially negative formulation of a right. Another simple definition was provided by Geoffrey Robertson in 1993 when he suggested that the right to privacy is, at its most basic and generic, "the right to be able to live some part of life behind a door marked 'do not disturb'"[8].

Definitions prove over simplistic to such an extent as to be unwieldy. Privacy by its nature means different things to different people and it is therefore difficult to rely on a single interpretation. Rather than seek to pin the tail on the donkey with a single definition, it is perhaps more helpful to provide an overview of the principal aspects of privacy.

### *Informational Privacy*

Informational privacy concerns the collection, use, tracking, retention and disclosure of personal information. It increasingly incorporates elements of decisional privacy as the use of data both expands and limits individual autonomy.

Informational privacy includes data protection, but it is broader than this, and also includes more 'positive' informational rights, such as freedom of information.

### *Physical Privacy*

Physical privacy is almost never referred to as such: it is concerned with the protection from outside interference of the body, the physical self. Physical privacy is widely protected through both the criminal and civil law (rape, assault, battery, and so on). However, many issues which fall within its remit are not yet adequately legally covered: excessive strip-searching, genetic testing, biometric testing, drug testing and cavity searches.

---

[5] See http://news.bbc.co.uk/1/hi/uk_politics/6262455.stm

[6] At Schedule 2 (5) and Schedule 3 (7) Data Protection Act 1998.

[7] Cooley on Torts, 2nd ed (1888), p 29.

[8] Geoffrey Robertson QC, *Freedom, the Individual and the Law*, 7th ed., Penguin (London, 1993) p. 104.

Inroads into physical privacy may involve subsequent inroads into informational privacy, for example if results of a biometric test are kept on a database.

### *Spatial Privacy*

Spatial privacy concerns the setting of limits on intrusion into personal spaces. 'Personal spaces' may include not only the home and domestic environments, but also the workplace, one's car, and even public space, depending upon the context. This was recently confirmed by the European Court of Human Rights in the admissibility decision in *Martin v. UK*[9] The Government had unsuccessfully argued that covert surveillance of the applicant's home by video camera was not an Article 8 issue as the nuisance which the surveillance attempted to address was not private in nature, and the camera only recorded what would have been visible to a neighbour or a passer-by on the street.

### *Relational Privacy*

Relational privacy refers to the freedom to determine one's associations with others. Certain aspects of it overlap with decisional privacy, and it includes, but is not limited to, privacy of communications or 'communicative privacy'.

Relational privacy has a positive and a negative aspect: it includes both the freedom to associate with others (and determine the extent and nature of that association) and freedom from others.

Relational privacy is protected in certain respects by the law (for example, through the laws relating to trade union membership and the right to association or non-association), but it is also restricted in certain ways (for example, through limitations on who is entitled to marry).

The best-known subset of relational privacy is communicative privacy. Here the positive and the negative aspects can be easily illustrated. Communicative privacy means not only that people should not be able to read your mail or listen to your telephone calls, but also that your communications should not be interfered with. Pure communicative privacy is rare, as post, e-mails or telephone calls will often be interfered with in order to garner their content (ranging from the use of investigative targeted surveillance to the nonchalant perusal of letters addressed to others). There have been instances in which postmen dumped sacks of letters without delivering them, for example. No information was garnered, the substance of the communications was never checked, but the letters were never passed on; love-letters, bills and postcards sat undelivered, and the writers and recipients were none the wiser that their lines of communication had been interfered with. Communicative privacy is also concerned with receiving unwanted mail – interference with your seclusion, in grandiose terms, or, more likely, interference with your inbox. Harassment and spamming are thus linked to communicative, and so relational, privacy.

### *Privacy as a Context-Specific Right*

Privacy is context specific, is valued in different ways and has different weight in relation to competing values and policy concerns according to circumstances. There are few hard and fast rules, and it cannot be said that conversations which take place in a public street are automatically entirely public

[9] *Martin v. UK* (Application No. 38199/97), March 27th 2003, European Court of Human Rights (Admissibility); case note at [2003] E.H.R.L.R. 461.

and subject to wider dissemination, nor can it be said that conversations or actions which take place in a private home will always be entirely private and immune from any public scrutiny.

Just as privacy in different contexts is valued in different ways, people might similarly expect that in every context where privacy was highly valued the law would provide similar controls and safeguards. This is regrettably not the case in the UK, largely as a result of the piecemeal, inadequate, *ad hoc* system of privacy protection in existence.

# The Scope of Work

## Surveillance

Much of the work covered by this privacy study relates to the post September 2001 and July 2005 legal landscape in Britain. It is axiomatic that when societies feel under threat, at times of flux, fear and uncertainty, governmental powers are often quickly expanded and civil liberties can suffer. This has occurred throughout history and across the world at times of epidemics and wars, with the introduction of temporary, emergency measures and the use of prerogative powers by the Crown. 'Wars on terror', however, differ as there is no clear enemy to be defeated and 'temporary', 'emergency' measures can subside irrevocably into permanent governmental policies.

The right to privacy can be particularly vulnerable at such times. This has been evident in the legislative shifts which took place in response to 9/11, which deployed 'nothing to hide, nothing to fear' rhetoric at times of suspicion, and the view of privacy as a more 'individual' right, pitched against the collective 'interest' in public security from terrorist attack.

The Government's response to the July 7 attacks in London focused through the Terrorism Act 2006 on the creation of new criminal offences and strengthening of police detention powers rather than on privacy. However, much of the language used during the passage of the Identity Cards Act 2006 demonstrated a belief that an enhanced need to hold and share information is integral to national security. The years between 2001 and 2006 have seen a rapid acceleration in the surveillance society. Advances in technology mean that levels of surveillance would have increased in any event. However, the political environment allowed this development at greater speed than might otherwise have occurred.

Following the arrival of a new Prime Minister, this is an opportune moment to take stock and consider the context in which recent developments in intrusive and mass surveillance have occurred.

## Genetic Privacy and DNA

The United Kingdom National DNA Database (NDNAD) is proportionately the largest in the world. Nearly 4 million people have their DNA permanently retained on the NDNAD representing 5.2% of the country's population. To put this into context, Austria (the country with the second largest proportion of its population with DNA retained) has 1% of its population in its database [10].

The legislative framework permitting DNA retention has been changed several times in recent years. Where once permanent DNA retention was limited to a limited number of offences following

[10] See http://news.bbc.co.uk/1/hi/england/nottinghamshire/6209970.stm

conviction, it can now take place following arrest for any recordable offence [11]. This has allowed the DNAD to mushroom in size. Roll-out based on arrest has also resulted in the NDNAD disproportionately impacting upon young black men. Figures compiled from Home Office statistics and census data show almost 40% of black men have their DNA profile on the database. That compares with 13% of Asian men and 9% of white men [12]. Concerns have also been raised about the number of children on the NDNAD. Following a series of Parliamentary Questions from the Conservative MP Grant Shapps it emerged in early 2006 that approximately 24,000 children under 16 who had never been convicted or cautioned for an offence had their DNA permanently retained on the NDNAD [13]. Even this figure has been dwarfed by recent reports that the true total might be around 100,000 [14].

The growth of the NDNAD has led to fears that the government intends to introduce a compulsory universal national DNA register without having a public debate on its merits or desirability. The greater the proportion of the population on the database, the easier an eventual compulsory roll out becomes. Certainly if everyone were on the NDNAD then allegations that it is disproportionately impacting on young black men would fall away. Similarly the taking of DNA at birth from all would negate suggestions that the holding of innocent children's DNA was treating them as criminal suspects.

There has been little debate on the merits and implications of a national compulsory database. Compared with years of argument over the National ID cards scheme this has been effectively non-existent. This can largely be explained by the progress of the ID card Bill(s) through Parliament providing focus for debate and by the fact that the Government has stopped short of formally proposing compulsory DNA registration. However, the issue does occasionally arise, particularly on occasions where advances in DNA technology allow for the conviction of a person years after the original commission of a crime [15]. Debate arising from such situations is extremely difficult to balance. On the one hand it is clear that the extension of the DNA database has allowed for an extremely serious crime to be detected; a crime that would have otherwise remained unsolved. On the other hand is the apparently more abstract concern that the taking of DNA from all will change the relationship between individual and state and that everyone will be treated as a suspect. The problem in balancing the argument derives from the fact that the benefits of mass DNA retention can be shown in a very case specific manner. In terms of individual rights it is very difficult to argue against the limited impact upon a person that the taking of their DNA will have when pitted against such a benefit. What is more difficult to gauge however, is the wider cumulative societal impact that DNA retention will have. The section on DNA will attempt to suggest the appropriate boundaries of DNA retention.

## Privacy and the Media

The incorporation of the European Convention on Human Rights introduced privacy rights into domestic UK law. Much of the caselaw under Article 8 has involved litigation by public figures

[11] A recordable offence is generally one which is punishable by imprisonment. However, a number of other non-imprisonable offences such as vagrancy are also recordable.

[12] http://news.bbc.co.uk/1/hi/uk/6979138.stm

[13] http://news.bbc.co.uk/1/hi/uk_politics/4720328.stm

[14] http://www.dailymail.co.uk/pages/live/articles/news/news.html?in_article_id=457046&in_page_id=1770

[15] For example Graham Derbyshire, convicted in December 2006 for rapes committed 11 years earlier. http://news.bbc.co.uk/1/hi/england/lancashire/6183959.stm

against the press. As a consequence, the development of common law interpretation of privacy has revolved around high profile cases such as those of Naomi Campbell and Catherine Zeta Jones.

Media privacy is also an interesting area in terms of potentially clashing rights. There is often a natural tension between Article 8 and the Right to Free Expression contained in Article 10 of the ECHR. A series of decisions in 2006 and 2007 have developed the relationship between privacy, free expression and the law of confidence. However, as the chapter on media privacy will demonstrate, much still depends on case by case interpretation.

The work on media privacy differs from the other parts of this work. While other sections are primarily concerned with the relationship between the state and the individual, media privacy remains firmly in the realm of dispute between private parties. Liberty will traditionally approach an issue from the perspective of identifying the limits of legitimate state interference into the privacy of the individual. This approach is not appropriate for media intrusion. The media is not part of the state and enjoys the right to free expression.

At the heart of any consideration of privacy is the concept of balance and proportionality. Thus use of intrusive surveillance powers under the Regulation of Investigatory Powers Act 2000 (RIPA) balances privacy rights against the need to detect and prevent crime, protect national security and so on. While these are legitimate interferences into privacy they are not 'rights' in themselves. Free expression is different. It is a specific right within the human rights framework which itself can only be intruded upon for specific legitimate purposes in a manner that is within the law and proportionate to need.

This makes the content and thrust of the media privacy work different. We do not try to create a hierarchy of rights or make specific recommendations. Rather the approach is to set out the development of caselaw and then identify areas of concern or those which remain unresolved. The recommendations suggest a number of possible approaches without identifying any specific preferred option. This different approach reflects the problems experienced by the courts in squaring a very difficult circle.

## Structure

The intention is to allow this project to be taken as a whole or as a series of individual discussions. Those interested in mass informational surveillance might not have the same interest in media privacy. As a consequence there is a certain amount of repetition of key aspects of the legislative framework and so on. This is because we do not wish to assume that an analysis of, for example, Article 8 HRA contained in one section has been seen by the reader of another. In any event, some repetition is necessary as the relevance of legislation varies according to the context.

## The Legal Framework

### The European Convention on Human Rights

The European Convention on Human Rights (the Convention) was drafted after the Second World War and the UK became a signatory in 1953. The Convention provides protection for an individual's private life. Article 8 provides:

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

Article 8 is a qualified right. This means that even if the right to respect for privacy in Article 8 (1) is engaged, Article 8 (2) allows for circumstances in which this right can be curtailed. There are three requirements that must be satisfied before any interference can be justified. First, it must be in accordance with the law. This means the interference must have a proper legal basis, such as a piece of legislation or rules of a professional body. The law or rule must be understandable, detailed and clear enough to allow a person to regulate his or her behaviour.

The second condition that the interference must satisfy is that it must pursue an identified legitimate aim. The legitimate objectives set out in Article 8(2) are; acting in the interests of national security, public safety or the economic well-being of the country; acting for the prevention of disorder or crime; acting for the protection of health or morals; acting for the protection of the rights and freedoms of others.

These objectives are widely drawn and it will often be possible for an interference to be categorised as being in pursuit of one of these legitimate objectives, for example, telephone tapping for the purposes of investigation or prevention of crime. More difficult questions arise where there are competing interests at issue, such as balancing privacy rights against the right of freedom of expression in cases of publication of photographs or materials about a person's private life. In some cases it will be important to distinguish between a lawful interference in someone's private life in the public interest, as opposed to an unlawful one which has occurred merely because it is something in which the public might be interested.

Even if the infringement of privacy is in accordance with the law, and it is for one of the legitimate objectives, it must still be 'necessary' in order for it to be justified under Article 8. This is the third and most stringent condition that any infringement must satisfy, bringing in a requirement that the act must be 'proportionate'.

The requirement of proportionality is often colloquially described as 'not using a sledgehammer to crack a nut'. In essence, this means that the nature and extent of each interference must be judged against the end it is meant to achieve and any interference with your rights under Article 8 that goes further than is necessary may well be unlawful. For example, a blanket policy of excluding prisoners during examinations of their legally privileged correspondence was considered a disproportionate interference with their rights to privacy and correspondence under Article 8.

The more severe the infringement of privacy, the more important the legitimate objective in each case will need to be. In most cases, the interference will be judged against whether it meets a pressing social need, and the extent to which an alternative, less intrusive interference would achieve the same result.

## The Human Rights Act 1998

The Human Rights Act 1998 came into force on 2nd October 2000 and incorporates the Convention into English law. The HRA gives 'greater effect' to Convention Rights in two main ways:

- It makes it clear that as far as possible the courts in this country should interpret the law in a way that is compatible with Convention rights.
- It places an obligation on public authorities to act compatibly with Convention rights.

The HRA also gives people the right to take court proceedings if they think that their Convention rights have been breached or are going to be.

Parliament makes laws but it is the courts that have to interpret them. The HRA makes it clear that when they are interpreting legislation the courts must do so in a way which does not lead to people's Convention rights being breached. Moreover, the courts are now under a duty to develop the common law – the law which has been developed through decisions of the courts themselves – in a way that is compatible with Convention rights.

If the law is an Act of Parliament, the courts have no choice but to apply the law as it is, even though it breaches Convention rights. However, the higher courts (the High Court, the Court of Appeal and the House of Lords) have the power to make what is called a 'declaration of incompatibility'. This is a statement that the courts consider that a particular law breaches Convention rights. It is meant to encourage Parliament to amend the law, but the courts cannot force the Government or Parliament to amend the law if they do not want to.

The position is different for secondary legislation. Secondary legislation is law made under the authority of an Act of Parliament. Rather than set out detailed provisions in an Act of Parliament, Parliament will frequently give the power to make detailed laws to a government minister. The Act of Parliament will give the minister the power to make law but the law itself will be set out in regulations or orders. For example, most social security law is set out in regulations rather than in Acts of Parliament.

Where the courts find that an item of secondary legislation is incompatible with Convention rights, they have the power to strike the law down or not to apply it. This applies to all courts, not just the higher ones. The only circumstance where this is not possible is where the secondary legislation merely repeats a requirement of an Act of Parliament.

The HRA requires public authorities to act in a way that does not breach Convention rights. The HRA does not define the term public authority, but it is clear that bodies like the police, local councils and government departments and agencies are all public authorities. Private individuals and bodies will not be public authorities for the purposes of the HRA unless they are performing a public function. The issue of whether a person or body is a public authority for the purposes of the HRA can be difficult to determine [16].

[16] This is a complex issue beyond the scope of this report. However, a Liberty briefing containing further information is available at http://www.liberty-human-rights.org.uk/pdfs/policy06/definition-of-public-authority.pdf

## The Data Protection Act 1998

The Data Protection Act 1998 (DPA) implements the 1995 EU Data Protection Directive[17] and regulates the storage and use of information about individuals.

The DPA serves two principal purposes. It allows individuals to access information held on them by a data controller by way of a 'subject access' request[18]. While subject access is extremely important, it is not as relevant to this report as the other main function of the DPA. This is to set out the framework by which any controller of personal data must comply.

The DPA sets out eight guiding principles by which all personal data must be handled. To compress the wording of the DPA, personal data must be:

(a) fairly and lawfully processed, and in particular;
(b) processed for limited purposes, which purposes usually need to be notified to the individual concerned;
(c) adequate, relevant and not excessive;
(d) accurate;
(e) kept for no longer than is necessary;
(f) processed in line with individuals' rights;
(g) secure; and
(h) not transferred to countries outside the EEA and several other approved countries without adequate protection.

Under the DPA, all personal data must be fairly and lawfully processed. "Processing" personal data under the DPA means obtaining, recording, holding, transferring, or carrying out any operation on the data. Whether personal data has been lawfully processed is perhaps more readily ascertainable than whether it has been fairly processed. The DPA recognises that some types of data are particularly sensitive and places additional obligations for anyone processing sensitive personal data[19]. The DPA also sets out a number of exemptions which in many circumstances permit the processing of data without the need for reference to the data protection principles. For the purposes of this work the main exemptions are national security[20], crime and taxation[21] and journalism literature and art[22].

[17] Directive 95/46/EC http://www.cdt.org/privacy/eudirective/EU_Directive_.html

[18] Section 7 DPA

[19] Under S.2 DPA sensitive personal data covers racial or ethnic origin of the data subject, their political opinion, their religious or spiritual belief, whether on not they are a member of a trade union, their physical or mental health or condition, their sexual life and the record of any alleged or actual criminal activity or sentencing

[20] Section 28 DPA

[21] Section 29 DPA

[22] Section 32 DPA

# 2. Introduction to Surveillance

*"Two years ago I warned that we were in danger of sleepwalking into a surveillance society. Today I fear that we are in fact waking up to a surveillance society that is already all around us."*

**Richard Thomas, Information Commissioner, November 2006**

State agents collect, monitor and disseminate information about each of us on a scale that would have been unimaginable ten years ago. Whether desirable or undesirable, this is a statement of fact that raises issues about the changing nature of the relationship between the individual and the state. By its very nature, state surveillance is likely to impinge upon individual privacy. The extent to which it is justified is arguably dependant on a range of factors. In human rights terms these can be summarised by considering whether the intrusion is taking place within a legal framework; whether the surveillance is serving a legitimate purpose (such as the detection or prevention of crime or the protection of public safety) and whether the intrusion is excessive for the benefit sought.

The last of these points in particular is extremely subjective. There is still huge debate and disagreement over the effectiveness and levels of intrusion caused by mass surveillance techniques such as CCTV and the National Identity Register (NIR) in particular. It is also particularly difficult to establish that mass surveillance techniques violate the Right to Respect for Privacy in Article 8 of the Human Rights Act. By their nature they are light touch and wide impact. This means that they are not likely to have a seriously detrimental effect on an individual on a day-to-day basis. Once the NIR comes into existence, life for most will continue much as before. However, the cumulative societal effect of the increased levels of information held on all will be considerable. The framework created by the HRA is designed to provide legal remedy for the individual not society as a whole. As a consequence, while there might be individuals who are able to use human rights protections successfully [23], mass surveillance is not particularly vulnerable to human rights challenges through the courts. Nonetheless, the human rights framework described does provide a useful analytical tool for judging impacts upon privacy.

[23] Such as the Peck case at the European Court of Human Rights – see the section on CCTV

So how much have things changed in recent years? Upon waking up today it is unlikely any of us felt more subject to surveillance than we did yesterday. This makes the societal shift difficult for individuals to comprehend. Added to this is the fact that, by its very nature, much surveillance takes place without our being aware of it. Even that most obvious symbol of surveillance, the ubiquitous CCTV camera, is so often seen as to fade into the background. It is unlikely that many people register the fact that each camera will be recording their movements for the time they are in range. If we were to jump 10 years into the future however, we would most likely be able to identify some dramatic changes. We might even be surprised by the extent of public indifference to them.

In November 2006 the Office of the Information Commissioner produced its '*A Report on the Surveillance Society*' [24]. This provided a detailed and comprehensive analysis of the nature and extent of surveillance in 2006. Part of the report contrasts a week in the life of a family living in 2006 and 2016. The projection into the year 2016 imagined a society of Identity Cards, private security, mobility tracking and remote controlled spy planes. All the predictions are either the culmination of current plans or new generations and developments of existing technology. While far from the realm of science fiction, the world of 2016 imagines days spent in constant surveillance to a degree that makes uncomfortable reading for anyone concerned with values of privacy.

In order to gauge the nature and extent of surveillance in the present it is necessary to categorise two broad types. Reference has already been made to 'mass surveillance'. This can be broken down into mass informational surveillance (essentially databases) and mass visual surveillance (such as CCTV). These are not targeted at any particular individual but store information in anticipation of possible use at some future point. Of course this does not have to relate to crime or national security purposes. The justification for information collection and dissemination powers created by the Children Act 2004 to be contained on the 'children's index' was child protection. The proposed NHS central data spine of patient's records is intended to allow easier nationwide access to information for health service providers. This might be obvious but demonstrates the simple-mindedness of the often cited comment, 'nothing to hide, nothing to fear'. Conflation of privacy and criminality presumes that those who are not criminals do not need to place a value on their privacy. This is clearly nonsensical as it is difficult to imagine any situation where a person would be comfortable with unfettered access to his or her medical records or the information about their children that will be contained on the children's index.

The other main type of surveillance is targeted surveillance by agents authorised by the state. The legal framework permitting targeted surveillance is set up under the Regulation of Investigatory Powers Act 2000 (RIPA). RIPA identifies different forms of surveillance such as communication interception, the use of undercover operatives and the capture of communication traffic data. The Act creates differing authorisation procedures according to the type of surveillance, while secondary legislation lists those public bodies that can use each power.

The focus of targeted powers under RIPA is criminality. Many of the agencies who are authorised to use targeted surveillance powers are not 'policing' bodies. Local Authorities, food and fishing agencies, the Charity Commission and many other bodies have RIPA authorisations (although many of these only have less intrusive powers such as access to communications data). However, in

[24] http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf

principle these powers are intended for use in order to uncover some from of 'wrongdoing', even if this is a regulatory matter not coming within the scope of the full criminal law.

Recently there has been a tendency to combine mass and targeted surveillance techniques through 'data mining' or 'profiling'. These are the means by which innocuous mass data is processed to allow an indication of characteristics or tendencies that might be used to justify some further and more intrusive step such as targeted surveillance, investigation or use of search powers. Following the alleged attempted attacks on planes leaving UK airports in August 2006 there was debate about the extent to which racial and religious profiling of passengers might be justified in order to allow more rigorous searches of passengers and luggage. Similarly, following the July 2005 bombings there was debate about particular targeting of ethnic groups on the London Underground and elsewhere. Ian Johnston, Chief Constable of British Transport Police, attracted attention with his comments that his officers would not be searching "little old white ladies". Meanwhile following the alleged attempted hijacking of aeroplanes from British airports in the summer of 2006 the former Metropolitan Police Chief Sir John Stevens suggested that much greater use of passenger profiling would assist security. This caused concern among Muslim groups in groups in particular while Metropolitan Police Chief Superintendent Ali Dizaei said that this would effectively create an offence of "travelling whilst Asian". However so far there have no been specific formal developments towards anything that could be described as 'racial profiling' [25].

There is no simple dividing line between profiling and intelligence led identification. To an extent, some form of profiling will take place as a matter of course in the activities of the police and other agents such as Her Majesty's Revenue and Customs (HMRC; formerly Customs and Excise). For example, it is likely that HMRC will pay particular attention to passengers who fit the common demographic of a 'drug mule' travelling from locations identified as drug importation routes . To use this demographic as the sole basis for stopping someone would effectively amount to profiling. To take into account other indicators, such as behaviour or mannerisms consistent with trafficking drugs, is arguably intelligence-led identification.

The line between profiling and intelligence-led identification can be blurred when profiling individuals. However, mining of data to identify, is increasingly based on totally automated systems. An example of data mining would be the computerised analysis of innocuous information to see if it produces any anomalies that might indicate some sort of criminality. The July 2006 Home Office white paper 'New Powers Against Organised and Financial Crime' (Cm 6875) proposed wide scale use of data mining and an idea of the ways in which trials had taken place and how data mining might be used in the future.

> *"A good example of the sort of 'profiling' work we would like to see more of is an exercise carried out a few years ago by HM Customs and Excise. Parallel checks were made on VAT and excise databases with information from the licensing trade and information on building dimensions from Land Registry. This exercise outlined a number of businesses which were submitting records which all looked reasonable enough in their own terms, but when put together came up with a picture which was highly suspicious. In a large number of cases, turnover was being reported*

[25] Although as the section on ID cards points out later, profiling of some type might eventually prove to be an inevitable consequence of the creation of the NIR

> *which would have been physically impossible given the size of the premises, providing a strong suspicion of money laundering activity"* [26].

Data mining is perhaps an inevitable development in surveillance. As increasingly large quantities of information are collated it becomes difficult for human agencies to sift. As a consequence greater reliance on automated techniques will become necessary. The nature of data mining has the potential to bring it into conflict with data protection principles requiring all data to be lawfully processed, to be for a specific purpose, to not be excessive for that purpose, and not to be held for an excessive time. This is a relatively new area where the legitimate aims of criminal investigation (or any other purpose for which data mining is considered necessary) remain largely untested. As a consequence there has been little determination of how data mining might be DPA-compliant. However, it is likely that stringent safeguards including the proper anonymisation of raw data, and the time-limited and targeted use of data-matching practices would need to be in place before compliance with the current legal framework is possible.

It is difficult to undertake a fully comprehensive investigation into surveillance. The sheer scale and number of databases, along with constant advances in technological capability can make work seem quickly dated. The '*Report on the Surveillance Society*' mentioned earlier has provided as close to a complete study on the nature of surveillance in 2007. We do not wish to replicate this comprehensive overview. As a consequence this study will focus on three specific areas; the use of intrusive surveillance under the Regulation of Investigatory Powers Act 2000 regime; the creation of mass informational databases such as the National Identity Register created by the ID Card Act 2006 and the Children Index created by the Children Act 2004; and the use of CCTV. This covers what Liberty considers to be the three main areas of surveillance; targeted surveillance, mass informational surveillance and mass visual surveillance.

The focus is essentially on surveillance and information gathering carried out by the state. Discussion of CCTV does touch on private sector use but sections on targeted and informational surveillance are specifically public sector. However, private sector databases are becoming increasingly relevant to individual privacy. As a consequence it is worth including a few observations of recent developments.

Private sector databases are huge. According to the credit reference agency Experian there are '440 million consumer information records in Experian's database, which is the largest in the UK' [27]. The commercial use of data is a massive growth industry. Tesco's Crucible database is reputed to have constructed a profile of every person in the UK regardless of whether they have shopped there [28]. The information contained in it will then be sold to other companies. An increasing number of companies exist solely to sell data accumulated elsewhere.

Mass data collation and dissemination without specific consent would appear to be difficult to reconcile with data protection requirements. However, given the lack of awareness of consent and the general availability of information that can be collated it is relatively easy to remain DPA-compliant.

---

[26] http://www.homeoffice.gov.uk/documents/cons-2006-new-powers-org-crime/cons-new-powers-paper?view=Binary at Page 22

[27] http://www.experian.co.uk/business/products/DF.html

[28] See '*Tesco stocks up on inside knowledge of shoppers' lives*' http://business.guardian.co.uk/story/0,3604,1573821,00.html

In particular, the passing of information to a company can literally result in the signing away of data protection rights through the giving of consent. It is unlikely that many customers will be aware of the extent to which they are allowing their information to be passed on through the use of a company's services. For example, the following is taken from the terms and conditions for customers of Tesco's online services;

> *"Any information you provide to Tesco ("data") will be put onto the Tesco database and processed by us for marketing purposes, market research, tracking of sales data, and in order to contact you or send you publications. Tesco may also disclose the data within its group of companies and to its professional advisers and agents for the above purposes. By submitting your data to us you agree to our storage and use of the data."*

The huge scope for private collection and dissemination of personal data can make data protection safeguards seem insufficient. Once consent has been given, whether or not it is informed, the processing of data becomes far simpler. In the Tesco example above, consent to wholesale data processing is a non-negotiable consequence of signing up to their online services. It is debatable whether many of those who shop online with Tesco are aware of this. It seems the private sector is increasingly bypassing data privacy in a manner beyond that of the public sector. Even Government departments do not attempt to suggest that the providing of information to them in itself constitutes wholesale consent to pass that information on. If privacy protections and rights are to have relevance in the private sector, there is a need to review the operation and effectiveness of what constitutes consent.

In recent years the boundary between public and private sectors has blurred as a natural consequence of the Government's increasing reliance on private-sector franchising of traditionally public-sector roles including healthcare, transport and education. In privacy terms this private/public crossover will be increasingly pronounced as a result of population-wide mass data programmes such as the NIR, the Children Index and the centralisation of NHS patient records. Access to the NIR in particular will increasingly become relevant to the private sector as a likely consequence of function roll out. Eventually NIR interfaces might become as common in banks as in hospitals and libraries making private sector attitudes to privacy increasingly relevant to the growth and continuation of the surveillance society. However, for now it is the individuals' relationship with the state that is of greatest relevance to privacy debate.

# 3. Targeted Surveillance

## Introduction

As opposed to generalised systems of surveillance (situations in which the privacy of many individuals is affected by wide-ranging or universal schemes) this section looks at targeted surveillance. Targeted surveillance is distinct from mass surveillance in that it involves the use of specific powers created through legislation used against a particular individual or individuals. These powers require the existence of some evidence that a particular person or location is engaged in an activity (typically in breach of the criminal law) that justifies the use of the powers. The same definition and rationale exists for other traditional policing methods, such as the use of search warrants. However, this is not surveillance as the person subject to a warrant will be made aware of the existence of the warrant and the carrying out of a search. Surveillance, by its nature, requires that the subject should usually be unaware of the interest and activity of the authorities at the time the surveillance takes place.

As with all issues of surveillance undertaken by the state, civil liberty and human rights concerns focus on striking the proper balance in a democracy between the protection of society from real threats to its integrity and the need to preserve the very values that make a democratic society worth protecting: the rule of law; respect for the individual and the avoidance of arbitrary or unjustified interference with citizens' rights.

In the law enforcement field, the object of targeted surveillance is essentially to obtain criminal intelligence information, and in doing so the methods used are often more invasive than general surveillance. They include:

- *the interception of communications:* for example, telephones, e-mail and other internet-based communications
- *covert audio surveillance:* the use of listening devices ranging from microphones to laser beams
- *human covert surveillance:* the use of undercover agents with or without the use of other surveillance technology
- *tracking and tracing devices.*

Whilst using such methods to target individuals is not new, it is the emphasis on this as a key component of the "war on terror" which has spawned an array of new domestic surveillance legislation across the world since 9/11. A leading example is the US PATRIOT Act – the acronymic short name for the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* – enacted in October 2001. It has far-reaching provisions covering interceptions and access to personal information (including library, medical, education, internet, television and financial records) without the need for individual suspicion. Another example is China, where the response has been to develop the Golden Shield project described as an "all-encompassing surveillance network – a gigantic online database – incorporating speech and face recognition, closed-circuit television, smart cards, credit records and internet surveillance" [29].

At the same time as changes in domestic arrangements, there has been an emphasis on the need to provide global intelligence cooperation. At the European Union level this has been consolidated in the Hague Programme, adopted by Member States in November 2004. It, for example, incorporates the new concept of the "the principle of availability" which, as the organisation *Statewatch* [30] says, seeks to ensure that nothing stands in the way of direct and automated access to data held by the policing authorities across the EU.

Since the attacks of September 11 2001, the legislative focus on surveillance powers in the UK has not been to strengthen intrusive surveillance. This is mainly due the passing of the Regulation of Investigatory Powers Act 2000 (RIPA) the year before the atrocity. Instead, most of the 'anti-terrorism' measures have increased the state's ability to create or access mass informational databases or to create powers for use against individuals such as the internment of foreign nationals under the Anti-terrorism Crime and Security Act 2001 and the Control Order regime set up under the Prevention of Terrorism Act 2005.

## Article 8 of the European Convention on Human Rights

Precisely because the surveillance is targeted, the core questions of when and how it is used become even more critical. In general terms, Liberty believes that the use of such powers is an accepted and justified right of a state so long as they are compliant with human rights. As with general surveillance, it is therefore the protection of privacy as guaranteed under Article 8 that provides the governing framework for the regulation of such methods.

It means that there must be a clear basis in law with detailed regulations so as to cover especially those areas where the technology available is continually becoming more sophisticated. It has to be shown, in each case where the surveillance is employed, that a legitimate purpose is being served – usually in the interests of national security or for the prevention and detection of crime. The interference to the individual or individuals must be proportionate to the risk faced. This requires that particularly intrusive methods should only be used in the investigation of particularly serious offences, and when less intrusive methods are not available or are unlikely to succeed. Furthermore, the exercise of such powers must be subject to a system of checks and balances including independent oversight and access to an effective remedy for those whose rights are breached.

---

[29] China's Golden Shield : Corporations and the Development of Surveillance Technology in the People's Republic of China , Greg Walton, Rights & Democracy, 2001.

[30] http://www.statewatch.org/

## Regulation of Investigatory Powers Act 2000

Prior to the introduction of the Regulation of Investigatory Powers Act 2000 (commonly referred to as RIPA) there was a patchwork of laws permitting intrusive targeted surveillance that had been developed in an *ad hoc* manner over many years. This led to a widespread view, including within government, that there were gaps in statutory and procedural controls that rendered many of the surveillance activities unlawful in terms of Article 8 in particular. This was emphasised when the then Home Secretary, Jack Straw MP, introduced the RIPA Bill in March 2000 as "…A significant step forward for the protection of human rights in this country…We are trying actively to ensure that our system protects individuals' Convention rights, while recognising how vital such investigatory powers are to the protection of society as a whole. Striking the right balance in this area is an important responsibility of Government and of the Home Office in particular" [31].

RIPA regulates invasive surveillance activities through a framework of warrants and authorisations. It is intended to provide a HRA-compliant framework for targeted surveillance by requiring that authorisation can only be given when the activity takes place for a purpose set by the statute and when it is a proportionate means of doing so. This reflects the requirement for a 'legitimate purpose' and the need to be 'necessary in a democratic society' as required in Article 8 (2) HRA [32] needed to justify any inroad into the right to privacy.

The method of authorisation differs according to the type of surveillance. These will be considered in detail below but a brief overview is appropriate here. The most invasive form of surveillance, the interception of communications, requires the issuing of an interception warrant authorised by the Secretary of State, who must be satisfied that the issue is justified on proportionality grounds (which include the need to consider alternative means of achieving the objective). The interception of communications must also be for a legitimate purpose more restrictive than the full set of acceptable grounds set out in Article 8 (2). It can only take place in the interests of national security, for preventing or detecting serious crime, or to protect the economic wellbeing of the country.

Authorisation of access to communications data [33] is similar to the interception of communications in terms of necessity and proportionality. However there is no need for the authorisation to come from the Secretary of State. It is, instead, an internal process in which a senior figure within the body accessing the data will provide authorisation. There are also wider grounds of justification of the need for interception; again, these include national security, detection and prevention of crime and economic wellbeing. However, they also include the interests of public safety, the protection of public health, the assessment or collection of tax, duty, levy or other governmental charge, the prevention, in an emergency, of death, injury or damage to a person's health, or for other purposes specified by Parliamentary order by the Secretary of State [34]. It is worth noting that this list goes beyond the legitimate purposes contained in Article 8 (2) HRA, which does not make provision for

[31] Hansard HC Debs. vol.345 col.767 March 2000

[32] Article 8 (2) HRA provides that 'There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'

[33] Communications Data is the record (but not the content) of communications such as details of phone calls, emails and visits to websites.

[34] Section 22 (2) RIPA

the assessment or collection of government charges. The ability of the Secretary of State to expand the grounds also contrasts with the prescriptive nature of Article 8 (2).

The remaining forms of surveillance are intrusive surveillance [35], directed surveillance [36], and covert human intelligence [37]. Directed surveillance and covert human intelligence sources are authorised internally on a similar basis as access to communications data. This list of permissible purposes is also similar. The authorisation of intrusive surveillance is permitted to the same limited number of purposes as required for the interception of communications [38]. The list of those who can provide authorisation is similarly limited to the Secretary of State and a small number of others, such as a chief police officer. The Surveillance Commissioner (who provides oversight of the use of directed, intrusive and covert human intelligence by agencies other than the intelligence services, MoD and the military) must also authorise any non-urgent request.

The bodies who can apply for the different types of order are set out in 'RIPA orders' made through secondary legislation. As a rule, the more intrusive the level of surveillance, the fewer the bodies who have authorisation under a RIPA order. The least intrusive surveillance power, access to communications data, is authorised by the widest range of public bodies.

It was hoped that the introduction of RIPA would be an opportunity not only to address new technologies and practices but also to bring the legislation into line with modern thinking about the protection the law must give to citizens' rights in this sensitive area. Whilst the resulting Act represents an improvement on the previous law in a number of respects – particularly in taking a more open, rights-conscious approach to surveillance – it can nevertheless at the same time be seen as more insidious. As the legal academic Helen Fenwick commented at the time "…the scheme is riddled with avenues to the broadening of such power, to be explored by the executive outside the full Parliamentary process…The RIPA pays lip-service to proportionality whilst largely emasculating methods of scrutinising it. It is apparent that a statutory scheme which hides the operations it empowers largely from scrutiny, and which, for the most part, places power in the hands of the executive, while shrouding the citizens' complaints mechanisms in secrecy, fails to reflect those democratic values" [39].

It is clear that much will depend on the way in which the different agencies – from the police and the security services to local authorities and others with a law enforcement role – exercise the powers of RIPA in practice. Although as yet there is no independent research on its workings [40], the provisions of RIPA fall some way short of a sufficient assurance that the fundamental principles of Article 8 will be observed. In broad terms this is due to the sheer complexity of the legislation. The Court of Appeal has called it "a particularly puzzling statute" [41] and Lord Bingham in a House of Lords case described

[35] Such as the use of a surveillance device planted in a property or car.

[36] Such as the bugging of a public place or the use of external telegraphic or listening devices directed into a property.

[37] Such as informants and undercover officers.

[38] That is the interests of national security, the detection and prevention of serious crime and the economic wellbeing of the country.

[39] Civil rights: New Labour, Freedom and the Human Rights Act Dorchester: Longman (2000) p.415.

[40] Following a request by the Home Office, the Association of Chief Police Officers (ACPO) submitted a review in May 2005 which considers issues of process, governance and bureaucracy but this has yet to be published.

[41] W, R v [2003] EWCA Crim 1632 (12 June 200s) para.98.

it as "perplexing", noting that "the trial judge and the Court of Appeal found it difficult to construe the provisions of the Act with confidence, and the House has experienced the same difficulty" [42]. At the same time, the then Home Secretary, David Blunkett, referred to "this horribly complicated legislation" in a speech in 2004 when also emphasising the red tape that it has generated – which is not surprising as it has given birth to an unprecedented number of statutory instruments (over 30), ranging from the designation of public authorities for the purposes of intrusive surveillance, for example, to the conditions for the lawful interception of persons outside the UK [43].

In more specific terms, there is the possibility that two key principles of Article 8 will be overlooked in individual operations. First, the necessity for each use of a RIPA surveillance power to be clearly and unambiguously established and its scope strictly confined to the requirements of the investigatory aim it pursues. Second, that the decision-making process contains adequate safeguards to protect the citizen against excessive intrusion or other abuses of rights. These concerns are exacerbated by the use of broad and vague notions such as "national security" and "economic well-being" in order to justify the surveillance activities. This gives rise to a real risk that disproportionate surveillance will be authorised to take place, going beyond what is necessary to protect the public from harm, and that it will interfere unacceptably with political and other lawful activity that ought to go unimpeded in a democratic society. It is of particular importance that the investigatory system be seen to avoid any suspicion that intelligence operations are mounted against organisations and associations on the ground that their political views differ from, or their activities may embarrass, the government of the day.

## Interception of Communications

It was not until 1985 that the government introduced legislation regulating the interception of communications (The Interception of Communications Act 1985 or IOCA). This followed the judgment of the European Court of Human Rights (ECtHR) in *Malone v UK* in 1984. Since then, there have been huge changes in telecommunications technology and communications services, giving rise to new human rights concerns. RIPA has now replaced all previous legislation as the primary legislation regulating interceptions.

Part 1 of RIPA defines the offences of unlawful interception, sets out the circumstances under which they are lawful, establishes a system of authorisation and issue of warrants, and imposes restrictions on the use of intercepted materials. The law extends to public telecommunications systems and to private ones such as mobiles, pagers and e-mail over the computer networks.

The right to apply for a warrant is limited to a number of high-level officials of the security services and chief constables of police. It has to be shown that the warrant is necessary in that it is in the interests of national security or for preventing or detecting serious crime, safeguarding the economic well-being of the UK, or giving effect to the provisions of any international mutual-assistance agreement. The conduct authorised must be proportionate to that which it seeks to achieve and the information cannot reasonably be obtained by other means.

---

[42] Attorney General's Reference (No.5 of 2002) [2004] UKHL 40 para.9.

[43] Speech at the Police Superintendents' Association's Annual Conference September 2004 as reported on www.spy.org.uk. The Recommendations of the Bureaucracy Taskforce (PBISG), 10 November 2005 states: "RIPA Review completed and submitted to the Home Office. The review considered various aspects of RIPA, including unnecessary bureaucracy arising from inappropriate application of the legislation."

Interception warrants have to be authorised by a Secretary of State, usually the Home Secretary. In 2004 the Home Secretary issued 1849 warrants and a further 674 warrants continued in force from previous years. By way of comparison, the total number of federal and state wiretap authorisations in the entire United States in 2005 was 1773. This executive authorisation by a member of the government rather than a senior judge was a key issue raised by Liberty during the course of the Bill in Parliament and remains the principal sticking point about accountability of RIPA authorisation. The Government's argument against judicial authorisation was that authorising interception involves particularly sensitive decisions that are properly a matter for the executive, and that judges cannot reasonably be expected to make decisions on what is or is not in the interests of national security. While the ECtHR has not specifically required that the authorisation be judicial, it has, on several occasions, stressed the importance of it being so. In *Klass v Germany*, it said that "it is in principle desirable to entrust supervisory control to a judge"[44]. Likewise in discussing the safeguards offered by French law on interceptions, it placed considerable emphasis on the safeguard of prior judicial authorisation[45]. It is also the practice in a number of countries, including Canada, New Zealand, the United States and other EU member states.

The Interception of Communications Commissioner, who is a senior judge, provides post-warrant oversight by reviewing the applications and submitting an annual report to the Prime Minister, which is laid before Parliament without a confidential annex. In relation to the latter, Liberty has long argued that proper accountability requires greater transparency through the publication of more detailed annual reports. In countries such as Australia, New Zealand and the US, the law requires publication of the statistics on the effectiveness of the operations in terms of arrests, prosecutions and convictions, and their cost. This is relevant to determining the necessity and proportionality requirements of Art 8 ECHR when deciding on future operations.

Another key debate during the passage of the Bill was whether the historical bar to allowing intercept evidence to be admissible in criminal trial should remain. Liberty has never supported this absolute bar, which seems to have been founded on concerns for the protection of the security services' sources and methods rather the fairness of the trial process. The bar is a legal anomaly as the UK is virtually the only country to have such a ban[46]. Whilst the evidence obtained under domestic intercepts is inadmissible, that obtained under foreign intercepts can be used if this is in accordance with foreign laws. There are no fundamental civil liberty or human rights objections to the use of this material, properly authorised by judicial warrant, in criminal proceedings. Rules of criminal evidence will apply to ensure that evidence is not admitted in such a way as to unfairly prejudice the case. And if there are concerns over protection of the state's sources, then clearly established rules of evidence may be used, to allow disclosure to be withheld from the defence and public.

More recently, this debate has focused on the evidential difficulties in terrorism cases and the fact that some of the exceptional counter-terrorism measures – including that of control orders – are being justified on the grounds that obtaining sufficient admissible evidence to prosecute in terrorism

---

[44] [1978] ECHR 4

[45] *Huvig v France* (1990) at para.33: "The court does not in any way minimise the value of several of the safeguards, in particular the need for a decision by an investigating judge, who is an independent judicial authority…".

[46] The Republic of Ireland being the only other state in the European Union to have a similar bar.

cases is proving difficult. It seems that senior police officers, judges and even the former Attorney General now support the use of such evidence in court.

One of the requirements of Article 8 is that a person must have an effective remedy when the state has breached this right. Like previous intercept legislation, the Act provides for an Investigatory Powers Tribunal to rule on written complaints over all aspects of surveillance regulated by RIPA, other than where the activity complained against involves the security services. It receives about 150 complaints annually and until 2006 had not found a single contravention of RIPA or the Human Rights Act. Its predecessor also did not uphold a single complaint in its 13 years of operation. However, in December 2006 the Tribunal found that Chief Superintendent Ali Dizaei's telephone had been unlawfully tapped[47]. This was the first occasion the Tribunal had made such a finding.

One of the reasons for such a low success rate is that the Tribunal cannot investigate an interception which was not authorised by a warrant. It therefore provides no protection against unauthorised interceptions, which are considered to be a matter for police investigation, and yet there is no requirement for the Tribunal to refer these to the police. There are also concerns over the closed nature of the procedure. There is no oral hearing, only limited disclosure of evidence to the applicant, and no reasoned decision. The Act specifically excludes access to the High Court to test the legality of decisions. These factors, together with the record of never having upheld a complaint, give rise to a question as to whether the present system can provide an effective remedy.

As well as regulating the interception of communications, Part 1 of RIPA creates a single regulatory regime for public authorities to access communications data held by telecommunications companies and Internet Service Providers (ISPs). Communications data includes all information relating to the use of a communication service other than the contents of the communication itself. It therefore includes subscriber details, billing data, telephone numbers, e-mail addresses, web sites visited and, in the case of mobile phones, the location of use. Such data is increasingly and significantly detrimental to privacy rights since it allows a detailed picture to be built of a person's contacts and activities. The purposes for which such data can be retrieved are wide: national security, prevention of crime, economic well-being, public safety, public health, and collecting or assessing tax. No prior judicial authorisation is required; only self-authorisation by a senior person in the body seeking the data.

Similar powers were already being exercised by the police, intelligence services, Customs & Excise and Inland Revenue prior to RIPA. In fact it is estimated that, of the approximately 1 million requests being made to the telephone companies for information, these agencies made around 95% of them. However, in 2002 the Home Office put forward a proposal to extend access to many other public bodies. It was quickly dubbed a "Snooper's Charter" by the Guardian newspaper and other opponents, including Liberty, which said that the inclusion of a range of bodies from the Financial Services Authority and the Health and Safety Executive to fire, local and even parish authorities would allow vast numbers of officials to self-authorise access to communications data. The order was subsequently withdrawn, and the Home Office put forward a compromise that restricts access to those agencies who have some link to criminal investigation, and that limits the purpose depending on the nature of this role.

---

[47] http://news.bbc.co.uk/1/hi/6166063.stm

Alongside this debate on extending access has been the discussion over the length of retention of communications data. The 2001 Anti-Terrorism Crime and Security Act allow the Home Secretary to require service providers to retain communications data on grounds of national security or the prevention of crime[48]. This potentially meant that a range of additional bodies would be able to draw on a considerable body of information on an individual.

Data retention of this type raises issues of fundamental principle over what is a proportionate approach to protection of national security or prevention of crime. It involves the creation of a pool of personal data about millions of innocent people – against the majority of whom there is not the faintest suspicion of unlawful activity. The longer such data is held the greater concern over the proportionality of retention. The Government does not have *carte blanche* in determining the length of retention. All European Community (EC) member states are under an obligation to comply with a European Directive on the retention of communications data[49]. This directive allows considerable scope for member states to retain data for a period between six and 24 months. There has been a voluntary code of retention for communications service providers in operation for some time already. This allows for retention of 12 months. The Home Office recently published a consultation on implementation of the directive[50]. Its recommendation was that data retention remains at the current 12 month retention adopted in the voluntary code. The consultation conceded that a case for extension had not been made out and that to lengthen the period data is held would be disproportionate. This positive approach demonstrates that an appreciation of privacy and human rights concerns can and does guide Home Office consideration and could bode well for future debate over the use of RIPA powers.

## Certified Warrants

There is a further level of detail relevant to the interception of communications (although not to the accessing of communications data) that should be examined before consideration of other forms of targeted surveillance permitted under RIPA.

The warranting process for intercepted communications described so far mainly covers warrants naming either one person or a single set of premises as the subject of interception[51]. There is however a far broader interception regime also permitted. These are covered by Section 8 (4) RIPA which allows the Secretary of State to certify a general warrant in respect of external communications (i.e. those sent or received outside the U.K). This warrant is limited only in that the Secretary of State is required to be satisfied that the warrant is necessary in the interests of national security, preventing or detecting crime or to safeguard the economic wellbeing of the country. The trawling of communications clearly permissible under the Section 8 (4) certified warranting process is in stark contrast to that permitted for internal communications.

The use of mass interception through certified warranting for external communications is not a new concept and was catered for in IOCA. The purpose was to allow Government Communication

[48] The voluntary code of practice under this Act states that 12 months should be the maximum length of retention of data. Also an agreed EU framework document permits retention for up to 12 months.

[49] Directive 2006/24/EC

[50] http://www.homeoffice.gov.uk/documents/cons-eur-dir-comm.pdf?view=Binary
Consultation closed June 2007.

[51] Section 8(1) RIPA

Headquarters (GCHQ) to collect large quantities of external communication in order to allow computers to trawl for keywords that might indicate potential terrorist activity (such as 'bomb' or 'Semtex'). However, the nature of mass modern communication processes makes it impossible to separate internal and external communications which will often be carried though the same cable. This means that internal communications could be subject to the same type of trawling exercises used for external communications. Because of this Section 16 RIPA contains extra safeguards relating to certified warrants.

At face value the extra safeguards seem an appropriate mechanism for ensuring that certified warrants do not allow trawling exercises through internal communications. Section 16 (1) provides that any material subject to a certified warrant can only be examined if a) it has been certified as necessary to be examined for national security, crime detection or prevention, or economic well-being purposes b) the purpose of examination is not the identification of material contained in communications sent by, or intended for someone in the British Isles and c) the material has not been selected for examination by reference to such a person.

However this safeguard is not as robust as it first appears. Section 16 (3) provides an exemption from requirements b) & c) in the paragraph above if the Secretary of State certifies that examination is necessary by reference to a particular individual. This certification can last for up to 6 months [52].

RIPA is a notoriously complex piece of legislation and the sections relating to certified warrants are particularly Byzantine. However, the combination of Section 8 (4) certification coupled with Section 16 (3) exemption seems to create the framework for an interception regime covering communications within the UK without the need for specificity required for standard internal interceptions. If the Secretary of State decides that the examination of mass material from within the UK by reference to a particular person or persons is necessary for terrorism, crime prevention/detection, or economic well-being purposes then (s)he can authorise the same sort of automated mass sifting carried out by GCHQ relating to external communications.

The framework set out in RIPA is confusing and creates grey areas. In particular it is difficult to establish what parameters might be set to identify particular individuals from the mass of information available for examination. It goes without saying that the operational use of certified warranting is not subject to significant scrutiny. The current regulatory regime on interception of communications under RIPA gives little insight into the extent to which internal communications within the UK might be subject to trawling expeditions previously only considered legitimate and proportionate to communications from or to other countries.

Given the vagueness of the certified warranting process, it might be anticipated that the Interception of Communications Commissioner would pay particular attention to their operational use. However, this is not the case. None of the annual reports published since RIPA was passed have mention certified warranting. There might have been mention made in the confidential annexes to the reports. If so, nothing has entered the public domain. The operational use of certified warranting remains shrouded in mystery.

[52] Originally three months extended to six months under Section 32 of the Terrorism Act 2006.

## Other forms of targeted surveillance

Unlike interception of communications, other forms of surveillance activities were completely outside any statutory control prior to RIPA. In order to ensure human rights compliance, the Act introduced a complex system – mainly through different types of authorisation described earlier – that is based on the apparent intrusiveness of the particular activity. At the less intrusive end is "directed surveillance", where a person who is suspected of criminal activity is placed under covert surveillance in a public place as opposed to private property. In this case the warrant for surveillance is self-authorised by a law-enforcement agency, only requiring permission of a senior officer. Law enforcement agencies issued some 23,628 directed surveillance authorisations and other public authorities some 6,924 during 2005/06 [53].

One of the key concerns that Liberty and others raised at the time of the Bill was the lowering of controls where one party to a communication consented to its being intercepted. Known as "participant monitoring", it occurs when, for example, an informant or police officer is involved in undercover surveillance work. Under RIPA, this conduct is exempt from the warrant procedures and safeguards of intercepting communications and is only placed under the lesser controls of "directed surveillance". Critics have argued that this is insufficient, as the non-consenting person whose privacy is infringed is entitled to the same level of safeguard as any other person whose private telecommunications are being intercepted by a state agency.

Further up the scale is "intrusive surveillance", when a person is placed under covert surveillance on residential premises or in a private vehicle including situations in which a bugging device is used. This is a narrow definition, as it excludes professional and business relationships at the workplace. Inclusion of workplace surveillance into the definition of intrusive surveillance would bring it in line with a 1967 US Supreme Court ruling, which held that privacy rights "protect people, not places". Like directed surveillance, it initially requires agency self-authorisation at a senior level but then has to be approved by the Surveillance Commissioner before it takes effect. There were 435 intrusive surveillance authorisations during 2005/06, with no mention of any having been rejected [54].

"Covert human intelligence sources", or CHISs, are informants or police officers used as undercover agents, usually to establish or maintain a personal relationship with a suspected criminal. There were 4,559 CHISs recruited by law enforcement agencies during 2005/06 and 437 by local authorities for the same period. The authorisation is by the Chief Constable or a person of equivalent standing in other agencies.

In addition to these forms of surveillance, there is "property interference", the only surveillance activity governed by statute prior to RIPA. The Police Act 1997 authorised entry or interference with property as part of a crime investigation. This again only requires self-authorisation, other than in sensitive cases involving a home or hotel room, or where privileged material may be obtained; in those circumstances, the approval of the Surveillance Commissioner is also required. There were 2,310 such authorisations during 2005/06, with four being quashed by the Commissioner for failing to meet the test of 'necessity'.

---

[53] paras.7.2 and 7.3, Annual Report of the Chief Surveillance Commissioner for 2005/2006.

[54] para.6.6 *ibid*

The Office of Surveillance Commissioners[55] provides oversight of all authorisations and publishes an annual report. Several concerns have been raised since RIPA became operative in 2000, including lack of staff to undertake the supervisory task effectively. It is also important to note that the management of authorisations is an issue taken up in several of the reports. For example, in the report for 2004/05 there is mention of inadequate RIPA training and education, and of the possibility of operations exceeding the terms of an authorisation. The 2005/06 report says that most instances of unauthorised surveillance occur because those carrying out the covert procedures have not been told by their managers the terms of the authorisations. It states, "This can lead to unlawful property interference and intrusive surveillance, and represents a fundamental failure of management"[56]. Directed surveillance authorisations are given particular mention for the many instances where the applications for authorisation continue to confuse necessity, proportionality and collateral intrusion. This is compounded when inexperienced authorising officers do not authorise the particular activity applied for[57].

There have been several cases before the Court of Appeal that have raised aspects of RIPA surveillance. In one, the defendants appealed against the inclusion of evidence that had been obtained through intrusive surveillance devices in their offices and cars, and that was used to convict them of conspiracy to defraud the Inland Revenue. The CA upheld the conviction, finding that RIPA "provides sufficient statutory oversight for the purposes of Article 8 and its case law", although at the same time referring to the Act as a "particularly puzzling statute"[58]. In another case involving an undercover police operation, the Court held that there were serious breaches of both RIPA and the Code covering undercover agents in the process of authorisation, which resulted in their being unable to assess whether the undercover actions were necessary and proportionate. However, despite this, it held that the conduct was not so seriously improper as to require a stay of the prosecution.

## Encryption under RIPA

Part III of RIPA governs the investigation of protected electronic data and is due to come into force in October 2007. It permits law enforcement agencies to request encrypted material to be put into an "intelligible form", sometimes requiring that the encrypted key be handed over.

In response to the Home Office consultation paper on a proposed code of practice in anticipation of Part III's implementation, Liberty again reiterated its view that it remains troubled by the scope of the powers granted by Part III. It potentially affects a large number of entirely innocent users of computers, with serious implications for both the privacy and security of computer data as well as e-commerce more generally. In particular, Liberty remains deeply troubled by the provisions of s.53, which reverse the burden of proof and thereby undermining the presumption of innocence and /or the privilege against self-incrimination.

Despite these concerns, there were reasons to suggest that Part III should be brought into force. During debate over the need to introduce a pre-charge detention limit of 90 days for terrorism suspects, the police and government highlighted the difficulty of obtaining encrypted material as a

[55] http://www.surveillancecommissioners.gov.uk/

[56] paras. 5.2 and 5.3 *ibid*

[57] para.8.11

[58] R v Lawrence and others, [2002] Crim LR 584 (3 August 2001).

reason justifying extension. It follows that the introduction of Part III could be a useful tool in obtaining access. There are serious civil liberty implications of 90-day pre-charge detention and it is likely that, whatever the concerns about Part III, its introduction would have removed one of the main planks justifying extended time limits. Arguably in terms of being a 'lesser evil', the introduction of Part III (which of course has already been passed by parliament) could be of benefit. Unfortunately the introduction of Part III is coinciding with government plans to introduce legislation to further extend pre charge detention limits in terrorism cases so there is not even this limited justification for introduction.

## Conclusion

At the heart of the legitimate justification for intrusive surveillance is the issue of accountability. Even the most invasive surveillance requires nothing more than authorisation from the executive. The most 'independent' figure in the system is the Surveillance Commissioner who authorises non-urgent directed surveillance warrants. The Surveillance Commissioner is a post created by statute, appointed by the Secretary of State. What is sorely lacking from the targeted surveillance framework is independent judicial authorisation.

This lack of independent authorisation contrasts with surveillance in the United States. This is perhaps surprising as the US is often criticised for its cavalier approach to individual privacy. The scope of the PATRIOT Act was referred to earlier, while recent reports over tensions such as that between the EU and US over the extent of flight passenger data required by the American authorities can help create assumptions that the US pays scant regard to privacy[59].

Whatever one's opinion of the current US approach to privacy, constitutional safeguards against excessive intrusion seem powerful. Historically there has always been independent judicial authorisation at the heart of the US surveillance process. Any surveillance warrant against a US citizen needed (and still needs) to be granted by a court. Meanwhile, interceptions of communications to the US originating from abroad needs authorisation from a special Foreign Intelligence Surveillance Court. After the September 11 bombings, President Bush approved a scheme of self-authorisation of the interception of international communications. When the New York Times uncovered the story, the American Civil Liberties Union brought a challenge that resulted in a US Federal judge ruling in August 2006 that the programme of interception without a warrant was unconstitutional.

This challenge to international surveillance techniques, along with increasing use of mass data gathering with the US, has meant that the authorities have been under pressure to reassure the American public that there is no unauthorised domestic surveillance. In November 2006 Dana Perino, deputy press secretary at the White House, went on the record to say "There is no domestic surveillance [in the United States] without court approval"[60].

---

[59] One consequence of the September 11 bombings was that the US demanded detailed information on all passengers travelling there. As a consequence a Passenger Name Record (PNR) containing names, birthdate, credit card details and other identifiers has been created for each of us when we go the US. It now appears that an agreement between the UK and US governments means the information provided on Britons will go beyond even what is required on the PNR. Information about other transactions on the credit card used for payment and email addresses will also be provided to US authorities. See http://news.bbc.co.uk/1/hi/world/europe/5029258.stm

[60] http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm

The contrast could not be clearer. In the UK there is no independent judicial authorisation of intrusive surveillance. In the US, an attempt to subject a limited number of communications to surveillance without judicial approval is deemed 'unconstitutional'. The Investigatory Powers Tribunal cannot be said to provide a safeguard against improper authorisation as its role is to determine the legality of interception that has already occurred. Similarly, the Interception of Communications Commissioner reviews the operation and use of intercept and communications data access powers after the event. For all its complexity, its unwieldiness and notwithstanding the other problems referred to in this section, RIPA would offer a reasonably proportionate surveillance framework, were it not for this single fundamental deficiency.

Intrusive surveillance is by its very nature secretive. Without proper and independent authorisation of surveillance, no scheme can properly protect privacy and civil liberty, nor offer proper accountability. In his diaries, the former Home Secretary, David Blunkett, gave a frank account of how he feared he was suffering a breakdown as a consequence of the pressures he was under. He recalled: "My whole world was collapsing around me. I was under the most horrendous pressure. I was barely sleeping, and yet I was being asked to sign government warrants in the middle of the night. My physical and emotional health had cracked" [61]. Even if we were to have absolute faith in the ability of those who authorise surveillance warrants to ensure that they are only issued in accordance with human rights principles of necessity, proportionality and purpose, it is vital that proper independent scrutiny should be at the heart of authorisation. The fact that RIPA apparently allows scope for a single member of the executive with many more pressing demands on his time to sign surveillance warrants, including mass certified warranting within the UK, in the complete absence of judicial process demonstrates the need for reform.

So far the Government has not indicated any intention to move towards judicial authorisation of communication interception. Meanwhile the Conservatives have expressed concerns over the excessive use of surveillance powers but have not as yet committed to a lessening of executive control. There are however indications of growing political interest in authorisation mechanisms. In July 2007 The Joint Committee on Human Rights published a report on counter terrorism policy and human rights. The main focus of the Committee's report were proposals to increase pre-charge detention limits above 28 days in terrorism cases. However, the Committee also considered the regime for RIPA authorisation, concluding that 'RIPA be amended to provide for judicial rather than ministerial authorisation of interceptions, or subsequent judicial authorisation in urgent cases' [62]. While the tide might be turning, no change to RIPA can be guaranteed. It is, therefore, necessary to consider other means that might be used to regulate the use of RIPA.

The sheer volume of authorisation of the more widely used and widely available powers such as accessing communications data would make judicial regulation logistically unfeasible at the present time. In his final report before retiring from his post, the former Interception of Communication Commissioner Sir Swinton Thomas reported that over 439, 000 requests for communications traffic data were made in the period 1 January 2005 to 31 March 2006 [63]. His report was critical of the

[61] See for example http://politics.guardian.co.uk/blunkett/story/0,,1889881,00.html

[62] Counter-Terrorism Policy and Human Rights: 28 days, intercept and post-charge questioning. Nineteenth Report of Session 2006-07 at paragraph 161 http://www.publications.parliament.uk/pa/jt200607/jtselect/jtrights/157/157.pdf

[63] According to the report for 2005-6 there were 439,054 requests – http://www.ipt-uk.com/docs/HC315.pdf

number of mistakes made. There were nearly 4000 mistakes in total with 66 relating to interception of communications, a figure he describes as unacceptably high' [64]. However the report did not criticise the high number of requests for communications data. Instead the figure was referred to in order to point out that the number of mistakes as a proportion was comparatively small.

While the report did not seem concerned at the number of communications data requests, the media did. *The Times* was unimpressed and ran the story under the title '*Privacy row as checks on phones and e-mails hit 439,000*' [65] and a series of commentators expressed concern at the levels of interceptions [66]. Relying on media-led regulation through opposition is not the most confidence inspiring scenario. However, the fact that a wide range of media opinion sees intrusive surveillance as an issue worth reporting might hopefully encourage some limitation for the future. Self regulation by individual public body is difficult without guidance on appropriate use. We are aware of the use of guidance for the authorisation of higher level RIPA powers by policing agencies. However, we are not aware of the extent to which guidance is followed for lower level RIPA self authorisation by non policing agencies such as local authorities.

Limitation on future granting of communications data access is far more likely to be affected by public and media concern. The experience of the 'Snoopers' Charter' demonstrated this. However, any future orders are likely only to extend the number of existing bodies with communications data access power. This means that, at best, the number would not increase.

Limitations on the use of more invasive communication interception powers might potentially be achieved by unexpected means. Some benefits of removing the bar on intercepted material in criminal trials have been considered earlier. However, lifting the bar might have other consequences. There are two main grounds of opposition to removal. First that it would allow details of security and police interception methods into the public domain. Second that it would require transcripts to be provided to defence representatives. This is because the standard rules of evidence disclosure in criminal cases require all material, both incriminatory and exculpatory, be available to both sides [67]. Not all the evidence would have to be provided to the defence. Material that is security sensitive can be withheld through the Public Interest Immunity (PII) procedure. However, disclosure is likely to result in large quantities of intercepted material becoming available. This, argue opponents of removal of the bar, would be costly, time consuming and would delay proceedings. It is certainly difficult to argue that it would not add cost to cases where intercept material was used. Prosecution often follows months of surveillance resulting in a huge amount of material being gathered. Even if the prosecution does not intend to rely on much of the material it must still give the defence details of and (subject to PII) access to unused material.

Despite this, the overall impact of the bar being lifted on the criminal justice system will not be significant. A total of 2243 warrants were issued in the 15 month period covered in the Interception of Communications Commissioner's Report referred to earlier. This amounts to approximately 150

[64] ibid 29 page 14

[65] http://www.timesonline.co.uk/tol/news/uk/crime/article1409395.ece

[66] See 'Are you being bugged' by Duncan Campbell for example http://www.guardian.co.uk/g2/story/0,,2017615,00.html

[67] The rationale being that while some of the intercepted evidence to be relied on might indicate guilt, other sections may exonerate. The interests of justice demand that the accused is able to rely on such material.

a month. Many of these interceptions will not result in prosecution making the total number of cases where intercepted material would be available a very small proportion of the million or so annual prosecutions.

While not significant in terms of impact upon the criminal justice system as a whole, lifting the bar might have a noticeable impact upon the granting of individual warrants. The agency making the application or Home Secretary considering whether to grant it will know that the material gathered may well end up as evidence passed to the defence. This could act as a brake upon the number of applications made. It is inconceivable that an agency thinking of seeking authorisation would be put off if the investigation involved the possibility of a terrorist attack. However, an agency seeking authorisation for investigation into less serious criminal activity without a significant public safety risk might hesitate before seeking RIPA authorisation. In particular, there might be cause to think twice if other methods of investigation had already produced a body of evidence that can be relied upon in a prosecution. The current inadmissibility of RIPA warrants means that there is a temptation to use them as 'the icing on the cake' to see if they result in any new evidence leads or to new suspects. Knowing that the transcripts might be accessible to defence lawyers and might complicate proceedings could temper any temptation. Unless the prospect of amendment to RIPA rises on the political agenda, increased accountability may well be dependant on greater openness in other areas.

# 4. Visual Surveillance

## The position in 2007

The year 2007 is a good point to revisit the introduction of closed circuit television in the UK, to examine the current profile of public sector CCTV applications, to consider whether the original confidence and anxieties were well placed, and whether the remedies devised during that time have proved effective.

It is just over ten years since the then Home Secretary, Michael Howard, made the initial decision to commit substantial sums of public money to set up hundreds of public sector surveillance systems throughout the UK, making use of the untested medium of closed circuit television. The original aim was to establish public systems as a crime prevention and detection measure, run principally by local authorities, or through partnerships with the police, with an emphasis on public safety: "to reduce crime and the fear of crime" [68]. A frenzy of public investment followed in the years after Howard's decision, in parallel with the expansion of CCTV in the commercial sector. By 2006, the Information Commissioner could report the existence of a total of 4.2 million CCTV cameras – 1 for every 14 people [69].

It is hard to generalise about CCTV systems. Schemes have in common the use of cameras, but other factors may be unique: they have been established in town and city centres, shopping malls, car parks, residential and light industrial areas, parks, transport stations, schools, universities and hospitals. Evaluation has proved difficult too, depending on the type of records kept, the figures chosen for comparison, and locally distinct social, environmental and cultural factors.

Initially, as a result of concerns about civil liberties expressed by local councillors and organisations such as Liberty, the emerging industry relied upon voluntary codes of practice, published first by the Local Government Information Unit, and later by the security industry. The revision of data protection law provided the opportunity for the introduction of a code of practice, published in 2000 and the

[68] *The Impact of CCTV: fourteen case studies*, Home Office Online Report 15/05, 2005
[69] *A Report on the Surveillance Society*, The Surveillance Studies Network, ICO, 2006

responsibility of the Information Commissioner. With data protection requirements being the only applicable domestic law, and interpretations of the European Convention on Human Rights still emerging, the progressive expansion of CCTV in the UK has relied more on stretching the boundaries of what is acceptable to the public and politicians, than on meeting any testing regulatory standards.

Public acceptance, and perceptions of the success of CCTV systems in achieving the original objectives of managing crime, are unchanged, and support continuing use and expansion. What has changed is the nature of CCTV itself, the technology and potential and actual applications of camera systems far exceeding the terms of the original set of possibilities and constraints.

Early CCTV systems relied upon analogue recording on videotape, depended upon the contemporaneous activities of control rooms employing qualified staff, and focused on providing evidence to support prosecutions in the event of criminal activity being caught on camera. The key issues were the quality of the image obtained, the skills and standards demonstrated by operatives, the management of operation rooms, and controls on the retention and handling of tapes. With overt use of cameras, the importance of signage, in notifying people in public spaces of the presence of cameras, was also established.

Now, technology, and the uses to which it can be put, has moved on, and it is more appropriate to talk of visual surveillance than of CCTV. The key issues retain their priority, but additional problems are emerging. Digital recording has led to the development of face recognition systems and biometric recognition techniques capable of incorporation into public place systems. Other physical and behavioural recognition systems are also under development. Failures of technology, inadequate public understanding, and the need for safeguards and protection systems become more important as technology becomes more sophisticated, and surveillance systems can potentially be linked digitally to other databases.

These issues are not confined to public space surveillance. Cameras as a tool of traffic management systems are not new, and cameras are an integral part of congestion charging schemes. The move from videotape to digital recording expands the potential of camera systems. Hailing “spies that never sleep”, the London Evening Standard reported in March 2006 on the installation of “new digital devices (that) run 24 hours a day, 365 days of the year and are capable of catching vast numbers of motorists”. The system, which will reportedly involve a constant data stream from 50 cameras, was said by the London Safety Camera Partnership to already have had a deterrent effect on motor crime that can be measured by a reduction in road deaths[70].

Many local authorities are considering the use of Automatic Number Plate Recognition systems, a tool for tracking vehicles during or after a crime is in progress: initially this is being considered in connection with serious crime, but there are no technical limits to its potential application. There is a potential to link overt public surveillance systems with this capacity, with other digital databases for directed surveillance. At present, ANPR systems are not controlled as directed surveillance under the Regulation of Investigatory Powers Act 2000: this issue would have to be addressed before these linkages could be made. However, with this general expansion of capability, regulation of the processing and retention of data becomes ever more important.

[70] *Evening Standard*, 15 March 2006.

## The Regulation of Visual Surveillance

There are two potential dimensions to privacy in the context of visual surveillance, incorporating its *surveillance role* – the actual process of watching people, and an *informational role* – the capacity of systems to gather and produce records on individuals that may be kept and used for other purposes[71]. The ground-rules are to be found in Article 8 of the European Convention on Human Rights, which protects the right of the individual to respect for his private and family life, home and correspondence, with regard to the activities of public authorities. This right is qualified, to the extent that it can be restricted to the degree that this is necessary and proportionate in order to protect public safety, or to prevent disorder or crime. Public authorities have a responsibility to take positive steps to prevent the violation of rights, and must have supervision and accountability systems in place when introducing public visual surveillance systems.

While the privacy implications of the surveillance role have caused less concern to members of the public than might have been expected, possibly due to a number of well-publicised cases where CCTV has played a role in bringing offenders to justice, and have not been strongly argued to date, in practice there are a range of factors that responsible public bodies take into account. These include careful camera siting, and the provision of notices drawing attention to the presence of a scheme. The careful management and supervision of control rooms is also likely to be relevant to the *surveillance* aspect of privacy.

The experience of visual surveillance may have an impact on individuals: having a chilling effect on their willingness to take part in public activities, or behave freely in, or enter spaces covered by CCTV cameras. The presence of a large number of cameras, the sense of being continuously under surveillance, increases the risk of this reaction. The technical capacity of a scheme would also raise potential privacy issues if it recorded sound, for example, or allowed camera operators to speak to passers-by through loudspeakers. There is a need for clarity over the purpose and scope of individual schemes, to avoid imposing unnecessary restrictions on behaviour, something in which everyone has a common interest[72]. Unnecessary surveillance may also have an adverse impact on freedom of movement[73].

Most significant for the future regulation of visual surveillance, is *informational* privacy, that is, the processing and management of data. This area of privacy is more highly developed, and it is here that UK data protection law bites. The Data Protection Act (DPA) creates a framework which requires that personal data be processed in accordance with a set of principles that protect the individual and are the foundation of standards of data management that apply to the public and commercial sectors. Images of individuals captured by cameras may amount to 'personal data', and the actions of searching and cross-referencing images with other information for the purpose of identification of an individual will amount to 'personal data processing' for the purposes of the DPA and so must comply with the data protection principles. The filming, recording, storing,

---

[71] *The Human Rights Act and CCTV*, Colvin, M, Local Government Association seminar, 28 June 1999

[72] *A Report on the Surveillance Society*, Surveillance Studies Network, ICO 2006, at 45.2.2 It is argued that, "albeit an individual value and a human right, privacy is also a common value because all persons have a common interest in a right to privacy even though they may differ on (its) specific content"

[73] *Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance*, Article 29 Data Protection Working Party, 11750/02/EN WP89

adapting, transferring and viewing of images were all considered to be covered when the DPA was introduced, and the Principles became the foundation of a code of practice for CCTV, devised by the ICO[74].

Most important is the requirement for fair and lawful processing; this requires that data be processed for limited purposes and not in a manner incompatible with those purposes. This principle is behind requirements for signage and a range of control room practices in public visual surveillance systems. The processor of images (whether the public body itself or a security company contractor) is responsible for ensuring that processing is carried out lawfully. Where it has grounds, the ICO can serve a notice asking a data controller for information on its practices, and in extreme cases can obtain a warrant for inspection and take enforcement action.

## Durant v Financial Services Authority

Data protection legislation was not originally envisaged as covering camera operated visual surveillance, and before 1998 a conceptual stretch was made to demonstrate that it covered video recording. The emergence of digital methods, and changes in the law following the implementation of the European Directive[75], have meant that visual surveillance is becoming a more natural fit within the data protection regime, although a recent decision of the Court of Appeal[76] has rather curtailed this more positive trend. The issue in this case arose over the need to show the relevance of retained data, in order to make a successful application for access to records. In order for the data protection legislation to apply, information must comply with the definition of 'personal data' in the DPA.

The Appeal Court refused Mr Durant access to certain records in the Financial Services Authority's (FSA's) filing system connected with a complaint he had made against Barclay's Bank, on the grounds that it did not qualify as personal data. In order to count as 'personal data', and so be covered by the DPA, it must be information that affected his privacy, whether in his personal or family life, business or professional capacity. Mr Durant had not been able to show that the information was close enough to this standard. The tests should be, whether information was biographical in a significant sense, and whether the individual was the focus of the information on file. As a result of the Durant case, whether any particular piece of information is covered by the DPA, will depend on where it falls along a continuum of circumstances in which an individual might have been involved to a greater or lesser degree. The implications of the Court's decision for visual surveillance are particularly complex, and are still being considered.

The key question must be; how far does the scenario outlined by the court limit the degree to which data protection bites on the use of visual surveillance technologies?

The Information Commissioner's initial assessment was that this would depend on the use and capacity of the system. A Good Practice Note, issued in February 2004, distinguished between focusing cameras or examining recorded images looking for particular people or examining the

---

[74] *CCTV Code of Practice*, Information Commissioner, 2000.

[75] Directive 95/46/EC (OJ 1995 L281/31), on the protection of individuals with regard to the processing of personal data and on the free movement of such data led to the Data Protection Act 1998.

[76] Durant v Financial Services Authority [2004] F.S.R 28, CA.

behaviour of individuals, and recording general scenes without any incident occurring and with no focus on any particular individual's activities[77]. On that view, privately owned basic camera systems, that cannot be manipulated remotely and that produce video recordings that are only made available to the police investigating particular incidents, such as those maintained by small retailers, may no longer be covered by the DPA[78]. Many activities carried out by sophisticated town centre and commercial systems will still be caught, but some of the images they record will no longer be covered.

At the beginning of August 2007 the Information Commissioner issued a revised code of practice for consultation, with the aim of resolving this question as far as possible[79]. This consultation indicated that the ICO now regards the vast majority of CCTV usage is covered by the DPA. The only persons listed as exempt from the DPA are those who 'use cameras for limited household purposes'. The proposed code of practice sets out an appendix containing a checklist for small retailers indicating what steps they should take to ensure DPA compliance.

This common sense interpretation of the Durant decision offers greater protection for targeted individuals, and ensures the existence of safeguards that will have a more general impact on the management of surveillance technology. It appears to take account of the public value of privacy protection, as "a sustaining principle of a democratic society"[80], and of compliance with the European Directive, in providing an international benchmark for data protection in the UK. Nevertheless, while this is a positive approach it could still leave uncertainty. Small businesses might, for example, wonder why they are now required to comply with a regime from which they previously believed themselves exempt. It will be important that the consultation plays an important part in creating certainty on these issues.

## International comparisons

The complexity of experience in the UK makes it difficult to pin down with any clarity potential public interest implications in the operation of public sector visual surveillance. International comparisons are useful in identifying some common concerns, although it must be recognised that these experiences are subject to differing concepts of privacy, the uneven operation of international standards, differences in domestic laws and jurisdictions and different political and public sector cultures.

Significant distinctions in attitudes to privacy have emerged over the last decade that can be examined in the context of visual surveillance. Although this comparison necessarily focuses on *informational* aspects of privacy, concerns are also expressed internationally on *surveillance* aspects of privacy.

The American Civil Liberties Union (ACLU) reports a weakening of privacy and loosening of the regulation of government surveillance in the United States. In the context of visual surveillance, the

---

[77] *CCTV Systems and the Data Protection Act 1998, Good Practice Note on when the Act applies*, ICO, February 2004 http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/cctv_system_and_data_protection_act_-_when_the_act_applies.pdf.

[78] This initial view stated that 'small retailers would not be covered [by the DPA] who, only have a couple cameras, can't move them remotely, just record on video tape whatever the cameras pick up, and only give the recorded images to the police to investigate an incident in their shop'.

[79] http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/ico_cctv_consultation_draft_final.pdf

[80] ICO 2006

ACLU highlights the lack of limits or controls on camera use. It picks out a lack of consensus on limits for the capability of public CCTV systems, and the lack of legally enforceable rules for the operation of such systems as particular causes of concern. The Washington police department's new video surveillance centre is capable of increasing the quality of technology and number of cameras, and according to the ACLU critique, is in danger of evolving into "a surveillance monster". Facial recognition is also a cause for concern. Constitutional protection exists, but clear and enforceable rules are needed, identifying what is expected of public bodies, and providing enforcement measures and punishments for violations[81].

By contrast, in 1998 the Government of New South Wales (NSW) Australia introduced a Privacy and Protection of Personal Information Act[82], providing a comprehensive framework of standards. The legislation is the basis of thorough cross-departmental guidance on the application of the Act to visual surveillance, aimed at local authorities, incorporating prior consultation, a set of guiding principles, practical guidance and explanation of enforcement measures and offences. New Zealand's (NZ) police have developed a policy on crime prevention cameras in public places. Much less detailed than that of NSW, this guidance also requires a degree of prior public consultation and gives a right to review public schemes to the NZ Privacy Commissioner.

European countries share common standards of privacy, in the European Convention on Human Rights, and the EU Directive on data protection[83]. Attempts have been made in several countries to address the informational aspects of visual surveillance, while also engaging with the public to gain support and consensus[84]. In Germany, arguments against CCTV are considered fairly weak, as by implication those caught on camera have entered an area where notice of the existence of cameras is clearly displayed. The German constitution protects a sophisticated multi-layered concept of individual privacy, but this has been moderated by legislation permitting CCTV schemes. This legislation does however require that the purpose of any CCTV scheme be established, and requires promoters to identify evidence to support assumptions about the risk of offending in areas where cameras are to be introduced. As a result, the police are reported as having exercised caution in establishing new schemes.

Other EU countries with specific enabling legislation, requiring prior consultation, public decision-making, and enforcement frameworks include Sweden and the Netherlands. Sweden has adopted a licensing system for public sector CCTV, with decisions made by county administrative boards, on the grounds of crime prevention and detection. A scheme of inspection is not working well, but the system is regarded as workable if given sufficient investment of resources. Sweden's system also places significant limits on the technology that can be applied. In the Netherlands, in what is described as a comprehensive regulatory scheme, public authorities apply to the municipal council, and are required to show a closely defined purpose for their proposals. CCTV systems are subject

---

[81] *What's Wrong With Public Video Surveillance?* ACLU 2002, http://www.aclu.org/privacy/spying/14863res20020225.html (11.09.06)

[82] http://www.austlii.edu.au/au/legis/nsw/consol_act/papipa1998464/

[83] References to these instruments, and summarised information about the approach to CCTV in a number of European Countries, can be found in *Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance*, Article 29 Data Protection Working Party, 11750/02/EN WP89

[84] All information making comparison with EU countries is drawn from *The Legal Regulation of CCTV in Europe*, Gras, M.L., in *Surveillance and Society, CCTV special, (eds. Norris, McCahill and Wood)*

to review, ultimately by the Data Protection Board which has a duty to supervise and powers of inspection. Complaints are made to a local council or a court.

These experiences illustrate the value of specific safeguards, even where these are in addition to constitutional provisions protecting privacy. In the US, the ACLU is running a "camera campaign" for legislation to regulate the use of visual surveillance. The dramatic expansion of capacity is another common theme, with Sweden going so far as to impose technological limits. Regulatory schemes appear to be most advanced in those countries that have either adopted privacy legislation, or have introduced specific legislation permitting CCTV, and incorporating requirements on its introduction and management.

Public opinion will be an important factor in determining the future direction of CCTV in the UK. It is particularly significant at present, as the coming year may represent a critical point in the application of public space visual surveillance systems in the UK. The Crime Reduction Delivery Board has been commissioned by the Home Office to prepare a national strategy for CCTV[85]. As stated earlier, the ICO has also launched a consultation on the revised code of practice. The debate generated by these initiatives will take place in the context of a demand for further massive public investment, to replace outdated analogue video systems, many of dubious value, with digital technology.

Public support for CCTV has apparently been sustained throughout the last decade, despite a lack of evidence that it is effective in reducing crime, or is having an impact on the fear of crime. The apparent lack of informed public critical concern about potential privacy issues indicates that there could well be a lack of balance in any public discourse.

It is clear that the government money invested in public space CCTV has produced mixed, even poor, results. Home Office case studies published in 2004 led to the conclusion that, "At best CCTV can work alongside other measures to generate some changes, but it is no easy panacea, and there is a lot still to be learnt about how to use it to best effect"[86]. These fourteen studies showed variations in whether schemes had had an impact on fear of crime, indicating no reduction in town centre areas, but reductions in some but not all residential areas examined. As in past evaluations, there are inevitable difficulties in evaluating and drawing conclusions from schemes with individually distinct characteristics. In general terms, it has also been suggested that caution should be exercised when considering and drawing conclusions from reports of opinion research on surveillance and privacy[87].

The ICO sought to draw out more considered and informed opinion by conducting a series of discussion groups with carefully selected members of the public, to provide the basis of policy recommendations to government on the future management of visual surveillance technology[88]. It emerged that public sector CCTV is perceived as benign, an anti-crime measure that brings benefit to individuals with few disadvantages of which people are conscious. Another relevant factor in public support for CCTV is trust in authority, and a genuine belief in the fairness of the system of law

---

[85] *Time for a new plan?* In CCTV Image, the official publication of the CCTV User Group, Summer 2006, www.cctvimage.com/downloads/CCTV_Image_16_Summer_2006.pdf [20 December 2006]

[86] *The Impact of CCTV: fourteen case studies*, Home Office Online Report 15/05 2005, at p36

[87] Haggerty, K.D, & Gazso, A., *The Public Politics of Opinion Research on Surveillance and Privacy*, in *Surveillance & Society 3(2/3): 173-180*. The authors advise caution over response rates, and critical scrutiny over how surveys are constructed and interpreted.

[88] *Public attitudes to the deployment of surveillance techniques in public places*, ICO March 2004

enforcement and criminal justice. CCTV in public places, particularly where notices are displayed, is not generally thought to intrude on personal privacy, a concept associated with the home. Further discussion showed that people also believe that privacy applies to their conversations, financial information and personal whereabouts, and for many people incorporates a sense of protection of personal dignity and personal integrity. Support weakens when considering the application of potentially more intrusive surveillance technologies, when the balance of elements of personal protection and potential disadvantage to the individual tipped away from the benign protection offered by CCTV.

Overall, the ICO research found that, before people were presented with the opportunity for more informed and deeper thinking about the impact of visual surveillance, there was "a general unquestioning assumption that CCTV works", and that despite qualifying this from recalled experience, confidence in public systems remained strong. Positive claims for CCTV in the media could be recalled, but no-one was able to cite stories to the contrary. A sense of personal protection has been created in areas covered by cameras, particularly when these involve real time recording, allowing immediate police or local authority response. However, this confidence does not extend to more intrusive surveillance technologies.

There is no reliable information available on the public response to new ventures, such as the attachment of loudspeakers to CCTV systems in public places [89], or the proposed use of microphones in connection with cameras in the security infrastructure for the Olympic Games in 2012[90]. The detail of these and other technological advances may challenge the non-specialist, but, as the Article 29 Working Party has observed, "the growing proliferation of video surveillance techniques can be easily appreciated by all citizens"[91]. Yet it does appear from the ICO research that public opinion in general is not fully informed. A focus on reports of the successful identification of those responsible for crime masks a much more complex situation in which individuals have a wider interest. As noted by the Working Party, "the development of available technology, digitalisation and miniaturisation considerably increase the opportunities provided by image and sound recording devices, also in connection with their deployment on intranets and the Internet. These are dimensions on which the ICO report suggests the public are likely to have opinions"[92].

## Misuse of surveillance data

Even when the potential for misuse of surveillance images is drawn to people's attention, their confidence is unlikely to be shaken: "they still tend to fall back on their own experience, which tells them that in real life the risks arising from CCTV are small, whereas the potential benefits are seen as very great"[93]. In fact, the number of reported instances of abuse leading to prosecution on the

[89] It is reported that seven CCTV cameras in Middlesbrough town centre now have a sound facility which allows operatives to give advice or intervene in incidents as they happen. http://www.middlesbrough.gov.uk/ccm/content/news/middlesbrough-council-press-releases/youve-heard-nothing-yet-cctv-wired-for-sound.en 27.07.06 [20.12.06]

[90] The BBC reported as controversial a proposal to use high-powered microphones on crowds at the London Olympics, http://news.bbc.co.uk/1/hi/uk_politics/6186348.stm [20.12.06]

[91] Article 29 Data Protection Working Party, 11750/02/EN WP89

[92] http://www.statewatch.org/news/2004/mar/wp89-video.pdf

[93] ICO, 2004 all references to ICO research on public opinion rely on this report.

part of public sector operating staff represents an incalculable fraction of actual camera operating hours. The most recent is the reported imprisonment, after trial on charges of voyeurism and misconduct in public office, of two CCTV workers from the control centre for Sefton Council in Merseyside. Images of a young woman undressing, bathing and using the toilet in her home, overlooked by a camera, had been displayed onto a plasma screen at the centre[94]. The charges of voyeurism did not succeed against all three defendants, emphasising the importance of enforceable standards of conduct in managing public sector surveillance. The control room itself was under camera surveillance, one of a number of measures available for monitoring control room operations.

Another cause of professional concern, the risk of false identification associated with visual recording, exacerbated by image quality, was reflected in the personal experience of people taking part in the ICO study. Despite this, support remained strong. Resistance was found mainly among young people, although infrequently. Suggesting that this might be attributed to an imperfect grasp of the technical capacity and remit of surveillance systems, the report acknowledges that, "Surveillance therefore seems to be capable of abuse, in terms of unjustified harassment – especially to those from minority communities". This perception appears to have led Asian and Caribbean young men to draw conclusions about the need for 'watching the watchers', prior consultation, and some privacy rules, although these measures received wider support, as did some form of licensing.

The abuse of surveillance equipment for intrusive purposes or harassment will amount to unfair processing, and breach of the First Data Protection Principle. For individuals, this will incur disciplinary sanctions, and for system controllers, attract the enforcement provisions of the DPA. The general law may also apply, leading to criminal prosecutions as in Merseyside. Effective sanctions are needed to underpin the DPA, and should be kept under constant review. In 2006, the Information Commissioner called for the penalties on conviction for offences under the DPA to be increased, and to include imprisonment, in order to deter the illegal disclosure and sale of personal information exposed by the ICO in its report, '*What Price Privacy?*'[95].

## Options for the future

The UK has developed a regulatory system for visual public sector surveillance technologies which, in comparison with some other jurisdictions, particularly in Europe and New South Wales, provides relatively weak 'constitutional' guarantees, but has resulted in relatively high management standards in the public sector, and has maintained public support. There are clearly complex reasons for international variations, but the power exerted by public awareness appears to be a critical factor in ensuring that standards are effectively enforced[96].

In the UK, despite confidence in public place surveillance, people are not well-informed about its regulation, despite the Treasury commitment involved. A number of desired rules emerged from the ICO study, including the need for signage, good quality images, a requirement for corroborative

---

[94] *Peeping tom CCTV workers jailed*, http://news.bbc.co.uk/1/hi/england/merseyside/4609746.stm (04.08.2006)

[95] *What Price Privacy?* ICO 2006

[96] *Declaration of the Article 29 Working Party on Enforcement*, EU 12067/04/EN WP 101, where it is noted that under-resourced and patchy enforcement regimes in some member countries may be attributed to an apparently low level of knowledge of their rights among data subjects.

evidence before individuals were apprehended, secure data retention, and operator training and supervision. Individuals should be protected by the need for consent for disclosure of images, and be able to obtain redress readily. With the exception of the evidence proposal, these are factors within the remit of the data protection regime, and to different degrees reflected in the existing code of practice. The new draft code, still at consultation stage, does seem to be attempting to strengthen and address some of these outstanding issues.

Other regulatory options, that appear to be attractive to the public, are beyond the powers of the Information Commissioner, and the *informational* aspect of privacy, and appear to engage more directly with Article 8, and *surveillance* attributes. They go beyond the protection of individual interests and raise complex questions about the accountability of the public sector in the use of visual surveillance, and its role in monitoring other uses of visual surveillance. These options include a system of licensing, a role for local authorities in granting permission for the siting of cameras in public places, and consultation and participation by local people in the decision whether to install cameras and where to place them. Privacy or surveillance impact assessments may also have a role to play[97]. Such options are incapable of implementation without further public discussion and the development of consensus. Public awareness is needed to raise the level of debate, and a forum in which those responsibilities that fall outside the remit of the Commissioner, but engage Article 8, can be explored and refined.

Three key questions emerge as we think of the future of visual surveillance technologies within the existing UK regulatory framework. The first is practical, and asks whether operators are meeting the requirements of the DPA, and maintaining signage, disciplined control rooms, and good data management and retention practice. The second encompasses the answer to that question, and asks whether the DPA is a sufficiently robust framework to enable the ICO to fulfil its role: "primarily to ensure that the Data Protection Principles apply in detail to the operation of surveillance in public places, and are seen to be properly and wholeheartedly enforced"[98].

The ICO lacks resources to build and promote its existing intervention, investigation and enforcement capacity, and can be expected to acknowledge that without general powers of inspection it is not possible to be confident that operators are complying with the legislation and code of practice. At European Union level, the Committee established to monitor the implementation of the EU Data Protection Directive[99] (the Directive upon which the Data Protection Act 1998 is based) is exploring what is needed for practical compliance, and seeking to harmonise compliance, has recognised that the ICO, along with its counterparts in other European countries, is under-resourced. But the ICO also needs sufficient powers. The Committee's call upon Member States to ensure that supervisory authorities take a more proactive step towards enforcement should add weight to this debate.

The further question addresses imminent developments in the form of technological advances in surveillance methods and data sharing, and asks whether the DPA framework can or should be the only tool with which we meet the challenge as a society. The answer here appears to be that there is

---

[97] *A Report on the Surveillance Society*, Surveillance Studies Network, ICO, 2006 where the potential of privacy and surveillance impact assessments are discussed in detail.

[98] ICO, 2004

[99] http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

a critically important role for the ICO in focusing the 'constitutional' implications of data management, taking account of Article 8, the Human Rights Act, and EU developments [100]. It will be necessary for the Commissioner to be proactive in asserting the need for safeguards, and enforceable codes of practice, as well as ensuring that essential incremental change is carried through.

## Debating the future of visual surveillance

It takes time for regulation to catch up with technological advance, and the need for a broad, well-understood national strategy, coupled with a regulatory system flexible enough to respond to change has never been greater. The ubiquity and general tolerance of CCTV cameras in daily life means that major changes in the nature of surveillance could take place without the public being fully informed and the implications properly tested. The use of digital techniques using biometric identification systems, and smart systems to track behaviour, as well as simple loudspeaker and microphone devices without informed consideration risk the occurrence of unforeseen and unintended consequences.

The unfettered expansion of technology has the potential to lead in the direction of startling cross-database applications of recorded material. Experience in other jurisdictions emphasises the importance of countries being able to rely on legislative, constitutional, and international standards. China's *Golden Shield Project* is an attempt to converge numerous technological applications in public sector infrastructure, banking and finance, and a range of public databases, as a matter of routine crime prevention and investigation. It has been reported by one writer that *Golden Shield's* aim is to integrate this gigantic online database with a surveillance network, incorporating speech and face recognition, closed circuit television, smart cards, credit records, and other surveillance technologies [101]. In 2003, the US Congress overruled an attempt by the Pentagon to introduce a scheme, *Total Information Awareness*, (later referred to as *Terrorist Information Awareness*), capable of interrogating multiple public databases, although the dismissal of this proposal has not quelled anxieties about future moves in that direction [102].

The Information Commissioner is the lynchpin of effective regulation. Some significant questions are posed as a result of current experience in this context, and must be resolved urgently: the ability of the Data Protection Act to regulate visual surveillance; the need for the ICO to have adequate resources to monitor and sufficient enforcement powers to take action over breaches of DPA requirements.

These questions do not however address the more fundamental issues for the future management of visual surveillance that are beyond the remit of the Information Commissioner. The expenditure of further huge sums of public money in updating schemes alone should increase the demand for

---

[100] Korff, D., & Brown, I., *UK Information Commissioner Study Project: Privacy and Law Enforcement*, Foundation for Information Policy Research, February 2004.

[101] *China's Golden Shield Project*, in Computing as a tool of governmental repression, Stanford University website making reference to *China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China*, Walton, G. at: http://www.ichrdd.ca/english/commdoc/publications/globalization/goldenShieldEng.html (04/08/2006).

[102] The defeat of the proposal is referred to in a New Scientist article, *Citizens Strike Back in Intelligence War*, 13 October 2003: http://www.newscientist.com/article.ns?id=dn4246 The ACLU had made a substantial submission to Congress: http://www.aclu.org/safefree/general/16854leg20030619.html (11.09.06).

greater accountability for the introduction and operation of visual surveillance schemes. Accountability goes further, however: the regulatory system itself needs to be reassessed. ICO research shows that people identify the necessity for a system of approvals and licensing when properly informed, and this option should be investigated. Consultation and participation in local decision-making, an essential part of current government plans for engaging local communities, should apply equally to CCTV. Decisions to renew, improve, or set up new schemes should be based on a locally agreed strategy, as already recommended to the Home Office as a result of its recent evaluation [103]. Local strategies should incorporate a risk and impact assessment that goes further than current perceptions of what is required, and takes into account the privacy impact of surveillance.

Any national strategy should take account of these issues, and incorporate a move to improve the regulatory framework. Before a national strategy is adopted, the Home Office, police, local authorities, and other stakeholders, must ensure that the continued use of visual surveillance is based on informed public support.

[103] Home Office, 2005

# Mass data retention: Identity Cards and the Children index

## Introduction

The holding of mass information though large scale databases is one of the most significant societal changes with privacy implications in recent years. The practice of targeted surveillance has been around for as long as there have been undercover operatives and basic surveillance devices. The use of CCTV is a more recent fixture but has been part and parcel of life since making such a dramatic impact upon the nation's consciousness following the murder of Jamie Bulger in 1993. Mass informational databases have also been around for decades. However, it is only in the last few years that their existence has synergised with everyday life. Fifteen to twenty years ago mass databases were generally the preserve of the police [104] or had specific purposes such as internal cataloguing systems used in libraries. Daily contact with mass informational databases was rare.

This has changed to such an extent that we experience on a daily basis the accessing of personal details though little more than the provision of our postcode. There is an inherent assumption that anyone providing a public or private service will have immediate access to relevant information via computerised access to a database. The regular use of Google and other search engines allows us to instantly access information about people and subjects that would have required hours of research only a decade or so ago.

Such changes mean that the passing of legislation allowing mass informational retention and dissemination with society wide impact has not always impacted upon the public consciousness. The Identity Card legislation was frequently in the news but, apart from those who were directly involved in debate, did not regularly feature as an issue of fundamental importance to the majority of the electorate. The Children's Index created by the Children Act 2004 attracted far less attention than this even though it introduced a mass informational programme of data accumulation and dissemination affecting every child in the United Kingdom and therefore, by extension, a good

[104] The Mark 1 Police National Computer (PNC) operated until 1992 and was then superseded by the PNC Mark 2.

proportion of the adults. Collectively these two databases will be relevant to every person in the United Kingdom who is here for longer than a temporary visit [105]. They will create a birth to death register of every person and allow for widespread access to this register. They are not the only two mass informational databases in the UK but they are likely to be both the most significant and controversial. The majority of this section will focus on the National Identity Register before a shorter consideration of the Children Index.

## The National Identity Register and Identity Card scheme

On 30 March 2006 the Identity Card Act 2006 (IDCA) received Royal Assent. The Government had taken four years, published two bills, spent millions of pounds and used countless hours of Home Office, Parliamentary and Committee time to pass legislation that will require the registration of everyone resident in the UK for more than three months [106].

At the heart of the Government's proposals is the creation of a National Identity Register (NIR). It is the NIR, rather than the ID card itself, that will have the most profound impact upon individual privacy. Indeed the card is more a by-product of registration. Focus on the card rather than the register has meant that public expressions of concern over the implications of introducing ID cards have been muted. Any waning of public support for the scheme can be linked more to concerns over cost and a growing awareness that the card will not provide the magic bullet solution to the problems the Government has claimed for it than to concerns over privacy. Most people are aware that many other countries have identity card schemes. Consequently there has been a presumption that the UK's proposals do not present any significant privacy concerns. There are two main reasons why such an assessment would be misleading.

First, no other common law country in the world has an ID card scheme [107]. A common law country is one where an individual's actions are lawful unless positively prohibited by law and where the courts are responsible for interpreting law. This contrasts with civil law countries (most European countries) which have codified legal systems. This is not in itself an argument against identity cards. However, it is worth noting that civil law countries tend to have far stronger codified privacy laws than the UK, which act as a balance against state intrusion into individual privacy.

Second, it is wrong to presume that all compulsory identification schemes are similar. The scope of the information sharing and dissemination powers contained in the Act goes far beyond those of other countries. The Act is also riddled with reserved powers allowing the Secretary of State to extend the scope of the scheme by Parliamentary order. This means that whatever the limitations imposed in the Act concerning what information is contained on the NIR entry, who is entitled to access that information and so on, these can increase dramatically over time. It is easy to see how such 'function creep' could be tempting. Following the conviction of Ian Huntley for the murders of Holly Wells and Jessica Chapman, the Bichard Inquiry was set up to investigate ways of ensuring that those who were unsuitable were not able to work with children or vulnerable people [108]. One of Sir Michael

[105] The Children Index will hold information on every person up to the age of 16 while the National Identity Register is planned to hold details of everyone above 16 resident in the United Kingdom for more than 3 months.

[106] Three months being the period the government has stated it intends to require registration.

[107] With the possible exception of Cyprus, which the Home Office argues is a common law jurisdiction.

[108] http://www.bichardinquiry.org.uk/

Bichard's recommendations was that an Independent Barring Board be set up to vet anyone who would not be suitable to work with the young and the vulnerable [109]. However, had an identity card been in place at the time it is likely that there would have been suggestion for 'soft' non-conviction information to be held on the NIR. There is a logic that once a scheme is in place and a further use is found, it makes both practical and financial sense to make as much use of it as possible.

The consequences of this were demonstrated by the wartime scheme. In 1950 a Parliamentary Committee looked at the use of the existing identity card and discovered that the original three purposes (conscription, rationing and national security) had mushroomed to 39 different functions. We can assume that whatever the initial proposal, this system would experience similar expansion of function and that the information held on the database will increase. It is worth noting that one of the first acts of the Conservative government in 1952 was to abolish the scheme. It was described by Winston Churchill as 'no longer necessary'. He went on to say that abolition would 'free the people'.

The privacy implications of the ID card scheme are profound. The proposed system will result in what the Information Commissioner Richard Thomas, when giving evidence to the Home Affairs Select Committee, described as a '*very significant sea change in the relationship between the state and every individual in this country*' [110]. Of course the IDCA does not by itself does not signal the death knell for individual privacy in the UK. However, it does symbolise a shift in the approach of the state towards the collection of information. It is arguable that we are moving away from a society where information is not shared unless necessary, towards one where it will be shared unless there is a reason not to. The Serious Crime Bill published in January 2007 gave evidence of this societal shift. It creates powers allowing information sharing and data mining by government departments with no need for suspicion or evidence. Although this will be limited to fraud purposes, the Bill tellingly contains powers to extend data mining powers by statutory instrument. This would provide a vehicle by which the practice could be extended to areas beyond fraud, or even for non-criminal purposes.

Public awareness of data sharing is poor. A MORI survey carried out for the Department of Constitutional Affairs in 2003 showed that 64% of people do not feel well informed about levels of information held about them, 74% don't know how to find out what personal information public services hold about them, while 53% don't know what their rights are regarding their personal information [111].

The post 11 September 2001 world was one where it became easier for governments to sell the idea of information collation as a necessary trade off for public safely. However, this could only partly explain why awareness of privacy issues seem, initially at least, to be confined to a minority. The manner in which the ID card debate was framed was an extremely telling insight into public attitudes to privacy.

---

[109] It is worth making the point here that Liberty believes that this proposal which became law in the Safeguarding Vulnerable Groups Act 2006 is sensible and desirable. At its heart is the recognition of the need to balance individual privacy against public safety.

[110] http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/130/4060805.htm

[111] *Privacy and Data-Sharing: Survey of Public Awareness and Perceptions* http://www.dca.gov.uk/majrep/rights/mori-survey.pdf

## Public Attitudes

Privacy experts are sometimes bemused by public indifference to privacy concerns. This lack of interest does not simply relate to the public. On 24 August 2006 *The Guardian* newspaper carried a news piece entitled 'Ministers plan to overturn key data protection principle'. The piece took up less than a single column on page 7 during the 'silly season' month of August when news of interest and relevance is thin on the ground. The article suggested that the Government was planning to remove one of the central planks of data protection in order to allow government departments to share information freely amongst themselves. This would appear to be in direct conflict with the second data protection principle in the Data Protection Act 1998 that '*Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.*' At the time of writing there does not seem to have been any specific attempt to take this proposal further. Indeed whether the removal or amendment of the second data protection principle to allow greater interdepartmental information sharing would be necessary is a moot point. As will be considered later in the conclusion which looks at the current legislative framework, it is arguable that the second data protection principle does not greatly limit modern mass data sharing capability. It allows for the sharing of data for 'one of more specified purposes'. If a wide range of purposes is specified by notification to the Information Commissioners Office, it will still allow broad scope for information sharing.

This lack of interest in informational privacy impacted on debate over ID cards. It was a peculiarity of the identity card debate that those who expressed concerns were put on the back foot by constantly being required by the media and elsewhere to justify their opposition. Usually when a Government is proposing a scheme that will have a profound impact upon the relationship between the individual and the state one might expect the Government to make a convincing case. Although justifications for introduction were given, the onus for explanation seemed very much on those expressing concerns to explain why they took issue. In other words the presumption was that there was no problem with ID cards and opponents had to convince people that there was.

In human rights terms the duty upon the state to explain why Identity Cards are needed is relatively straightforward. If it is accepted that the scheme will have some impact upon individual rights to privacy, then it should also satisfy a legitimate aim such as national security, the prevention and detection of crime, for the protection of public safety, the protection of health, and so on. It should also be 'proportionate' in that the scheme is the least intrusive way of achieving the desired ends.

There is little suggestion that the NIR scheme would be in breach of the requirements laid out in the Human Rights Act 1998 and the European Convention on Human Rights *per se*. Indeed as the scheme stands as passed it is extremely unlikely that the European Court of Human Rights (ECtHR) would find a breach of the Right to Respect for Privacy and Family Life in Article 8 of the Convention[112]. The ECtHR has tended to allow states considerable leeway with the principle of an identity scheme.

Of course the Government has put forward justifications for the scheme saying that it will help fight terrorism and unlawful immigration, deal with crime and fraud, and improve access to public services. The point is that public attitudes towards privacy mean a rights-based approach to identity cards does not seem to have held the Government to account.

[112] Whether the same remains true following likely future extension of information that can be held on the register and those who have access to it remains to be seen.

An extremely telling aspect of the debates on ID cards was the weakness of the justifications put forward for their introduction. Possibly the strongest argument in their favour is that entry on the NIR and possession of an identity card will improve access to public services. Even the scheme's most entrenched opponents could not disagree that a single identifier, which will be the point of entry, contact and verification, could be of assistance in gaining access to a range of public services from the NHS, to state benefits, libraries, and so on. However this hardly featured as a justification when the Government was selling the scheme. Instead the focus was primarily on helping fight terrorism and crime. As time progressed other reasons were put forward. These ranged from dealing with illegal immigration to combating identity and benefit fraud.

During debate on the Bill, Liberty and others argued strongly that none of these arguments stood up to any degree of detailed examination. It might be argued that there was the potential for the NIR and identity card to be of *some* assistance in providing solutions. However, few outside Government with any detailed knowledge of the scheme seemed at all convinced that the NIR was the most cost effective and least intrusive way of dealing with the problems the Government maintained would be solved. Many IT experts believed (and are still arguing) that the sheer scale and cost of the scheme make it unlikely to ever work. Liberty's Parliamentary briefings on the Bill explained its concerns over the effectiveness of the justifications, and there is no need to revisit these in any detail again[113]. It is, however, worth pointing out that even after the 7 July 2005 attacks in London, the then Home Secretary, Charles Clarke, accepted that ID cards would not have prevented the bombings. Tony McNulty, the minister in charge of the scheme, in the Autumn of 2005 admitted that they had 'oversold' the benefits of the scheme at a meeting of the Fabian Society. Such admissions were more widely reflected in the general change of tone adopted by advocates of the scheme. Rather than adopting the 'panacea' approach of the early days, emphasis was more on how the NIR as a whole would be one of several factors helping fight terrorism, crime and so on.

So why was the focus on keeping us safe rather than getting better public services? One practical argument is that access to better public services can only be a convincing justification for a voluntary scheme allowing people to 'opt in' if they so wish. However, the need for a commercially viable scheme meant there needed to be a take up rate that guaranteed a set and significant number of people every year. This could only be achieved through a compulsory scheme in which a certain percentage of the population would be expected to sign up every year.

Until the final stages of the Bill there was a power allowing the Secretary of State to require registration of groups of individuals identified by an order made in Parliament. This was removed as part of a 'compromise' in order to ensure the Bill was passed by the House of Lords. New legislation will now be needed before the Secretary of State can require registration. However, a lack of compulsion would have effectively ruined the Bill as only those who volunteered to register would be entered on the NIR. Because of this the Government insisted on keeping the power to require people to register when applying for other 'designated' documents[114]. The passport was identified as being the appropriate document as it guarantees that most of the population will need to renew (and therefore register on the NIR) every ten years. This led to a rather farcical situation. The Government claimed the removal of the Secretary of State's power to require registration made the

[113] All Liberty's briefings are available at www.liberty-human-rights.org.uk

[114] Sections 4 and 5 IDCA

scheme no longer compulsory. However, it had ensured that nearly 10% of the population would be required to register annually. This effectively provided the compulsion necessary to ensure the scheme might be financially viable.

Another reason for focusing on public safety rather than public services is that the scope and justification for information retention and dissemination would be much broader. The range of the NIR is likely to increase over the years as parliamentary orders permit the holding of increasingly sensitive personal data available to an increasing range of public bodies. Parliamentary orders usually avoid detailed scrutiny. Even so, it is easy to imagine growing disquiet among MPs and peers asked to agree to a growing number of extensions with privacy consequences when the underlying justification to the scheme was improved public service access.

## The Legislation

It should be stressed that the Identity Cards Act is enabling legislation. This means that the legal framework for the anticipated scheme is in place. We will consider some of the potential pitfalls and problems the scheme may face later on. However, given that the legislation has been passed, it is appropriate to imagine that the move towards ID cards might happen in a manner as envisaged in the IDCA.

# History

The genesis of the IDCA was a White Paper published early in 2002. *Secure Borders Safe Haven* announced that the Government would soon be consulting on plans to introduce an 'entitlement card'. In July 2002 'Entitlement Cards and Identity Fraud' was published. This envisaged a voluntary scheme essentially allowing the user to use the card in place of other forms of identification such as driving licences and passports and using it to allow easier access to public services. The consultation ran until January 2003. There was then little further progress throughout the year until November when findings of the consultation were published. The Home Office analysis was so positive that in fact a compulsory scheme was now proposed in the paper 'Identity Cards: The Next Steps'. This was slightly surprising, as compulsion had been specifically ruled out during the Entitlement Card consultation.

The draft ID Card Bill was published for consultation in April 2004. Responses to this consultation included a report from the Parliamentary Home Affairs Select Committee, which was supportive of the principle but critical of the detail of the Bill [115]. The Bill itself was published in November 2004. Few changes had been made. The Bill progressed through the Commons to the Lords, where it had its second reading in March 2005. The 2005 General Election then halted the Bill's further progress. Many commentators felt that the Bill's progression to this point had been largely dependent on the Government's huge Parliamentary majority. The Conservatives and Liberal Democrats opposed the scheme and several Labour backbenchers were unsupportive. When the 2005 election reduced the Labour majority from 161 to 65, there were rumours that there would be no attempt to reintroduce the Bill. These were quickly scotched by the then Prime Minister Tony Blair, who said that Identity Cards remained one of the Government's top priorities. A new Bill was therefore introduced to the House of Commons soon after the election in May 2005. The Bill again passed through the House

[115] http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/130/13002.htm

of Commons with little alteration but ran into concerted and sustained opposition in the House of Lords principally led by the Liberal Democrat Peer, Lord Phillips of Sudbury. This eventually led to the compromise described earlier, in which there could be no compulsion of any group without further legislation (although compulsion would still take place when obtaining a new passport). In the end, however, the Government effectively got its way. Many Peers had clearly become increasingly uncomfortable with continually blocking Government legislation. Meanwhile in the Commons, many Labour MPs had recently voted against the Government causing defeats in the Terrorism Bill and the Racial and Religious Hatred Bill passing though Parliament at the same time. Perhaps understandably, many were unwilling to further defy the party whip and thus the Bill received Royal Assent and became an Act.

## The Act

The Identity Cards Act 2006 is not a particularly lengthy piece of legislation. It contains 44 Sections and two Schedules. Considering its name, the Act contains remarkably few clauses about identity cards themselves. Liberty has maintained since the draft ID card Bill was published that the Government's plans were more concerned with the creation of the NIR than about the cards themselves, which are essentially a by-product of registration. This is borne out by the Contents page of the Act, which makes 11 references to the register but only five to ID cards themselves.

As no ID card has yet been produced and the NIR has not yet come into existence, comments about privacy repercussions must be based on the legislative framework creating the scheme. The purpose of this study is not to provide a detailed clause-by-clause analysis of the IDCA. This has been provided elsewhere by Liberty and others[116]. Rather, it will focus on the way in which the main provisions could impact upon privacy. This will not be limited to informational privacy, but also the impact that the fully operational scheme could have on individual privacy by, for example, potentially becoming a tool of internal immigration control. It is not possible to make an accurate prediction as to the full impact on individual privacy. What this work will attempt to do is draw attention to possible areas of future concern. As both the Conservatives and Liberal Democrats have pledged to scrap the scheme if elected it may be that the scheme never moves to full compulsion. Similarly, technical and procurement problems or cost issues may make the scheme unviable[117]. However, we are assuming that things progress according to the legislation passed and the stated intentions of the Government.

It should be emphasised that most comments will relate to the initial scope of the Act. Nearly every definition is attached to a power to amend by parliamentary order.

## The Register

At the heart of the Act is the NIR. The first five clauses set up the NIR and create the framework for registration. The two specific purposes of the NIR are to create a means for people to establish their identity and to allow a means for that identity to be checked when necessary in the public interest. This

[116] Liberty's briefings are available at www.liberty-human-rights.org.uk

[117] See the Sixth Report of the Parliamentary Science and Technology Committee http://www.publications.parliament.uk/pa/cm200506/cmselect/cmsctech/1032/103202.htm

is one of the few parts of the Act that is not subject to alteration by public order. However, the definition of what constitutes the 'public interest' is so broad[118] that the scope is already extremely generous. In any event there is nothing that would prevent extension through a future act of Parliament. Nearly every piece of legislation before Parliament will contain provisions amending an earlier act.

Section 1 also contains the list of what are known as 'registrable facts'. This is the information that will be held initially on the register. This covers some quite basic information such as name, current and previous addresses, date of birth. It also contains more intrusive data such as current and previous residential status and numbers allocated for identification purposes. Concerns over what might be included in 'numbers allocated for identification purposes' raised concerns during passage through parliament about what this could entail – identification numbers being used for a wide range of information. A limitation was put on this so that disclosure (but presumably not retention) of such information could not cover information defined as sensitive personal data within the meaning of the DPA. Actual information recorded in the register is set out in section 3 and schedule 1 of the Act and again can be modified by parliamentary order. As well as the information relating to registrable facts, Schedule 1 also allows identifying information to be held on the register. 'Identifying information' is categorised as a photograph, a signature, fingerprints or other biometric information

While the scope of information has been initially limited it is likely to expand. Indeed it could be argued that it must expand if the ID card scheme is going to achieve the aims the Government has in mind. A good example of this is the claim that it will help fight terrorism. As mentioned earlier, the former Home Secretary, Charles Clarke, publicly accepted that ID cards would not have prevented the July 2005 attacks. Given that a sophisticated terrorist network is likely to recruit those with no criminal convictions or history with the authorities, this must be right. It is also hard to see how their entry on the NIR would have given any indication that they might be a security risk.

In fact, it makes sense to assume that British intelligence and policing agencies have gathered information on anyone that they believe could constitute a risk to national security. The reality would be that anyone who does give reason for concern would become subject to a level of targeted surveillance that would collate information going way beyond what would be contained on the NIR. It is not feasible that the NIR entry would add to information already possessed by the Security Services.

This leads to two conclusions. First and most obvious, for the vast majority of people who are not involved in terrorist activity, their entry on the NIR will be irrelevant in combating terrorism. The second conclusion is more worrying. In order to be of any use whatsoever in combating terrorism the NIR *must* contain more information. This would need to be of a type that would separate those who present no or minimal risk to national security from those who might pose a serious risk. In other words, it would need to be capable of allowing some degree of profiling and categorisation.

Profiling has become a significant issue since the London bombings of July 2005. Immediately after the attacks, British Transport Police indicated that some sort of profiling of passengers on the London Underground might be necessary, a view initially endorsed by the then Home Office Minister Hazel Blears[119]. Similarly, following the alleged attempted attacks on planes flying from UK airports

[118] Being national security, prevention or detection of crime, immigration, employment prohibition, and provision of public services.

[119] http://news.bbc.co.uk/1/hi/england/london/4732465.stm

in August 2006, the issue of profiling air travellers was raised in response to the huge delays caused by searching all those waiting to board planes[120]. Profiling is a difficult issue in civil liberty, equality and privacy terms as it covers a broad spectrum of activity. There is a point on this spectrum when legitimate intelligence-led profiling becomes so general as to become profiling based on, for example, little more than racial or religious characteristics.

If a greater level of information were to be held on the NIR it would certainly have the potential to allow some degree of profiling. By its nature however, it would need to be of a general level identifying characteristics that might give reason for concern. Any specific information indicating that a particular individual was a risk would almost certainly mean that they would already have come to the attention of the police and security services.

This point is not being made in order to suggest that the NIR will inevitably be used for profiling purposes. It does however illustrate a difficulty for the Government. In order to make the ID cards scheme advance the ends claimed, it may well have to become far more intrusive.

Eventually it is intended that everyone be registered. Earlier versions of the Bill allowed for registration to take place by one of three methods; voluntary registration, registration required as a consequence of applying for a designated document, and registration through being one of a group of people determined by the Secretary of State. The ability of the Secretary of State to require registration was removed as part of the compromise to ensure the Bill was passed. The process for registration by volunteering or by passport application requires both the handing over of information to be used as well as the attendance at a specified place to provide biometric information. There are some practical difficulties that might arise from attempts to gather biometrics. The London School of Economics report on Identity cards identified a range of problems that could arise from a wide scale attempt to obtain biometric identifiers. An example being the large number of people in the UK from whom iris scans cannot be taken[121].

## ID Cards

Creation of the NIR is at the heart of the Act. Most of the privacy implications of the scheme flow from the information to be held on the register, powers to access that information and the data trail that will follow from accessing the register. It is of course the ID card itself that is of greatest interest to the public. No-one who is required to register as a consequence of applying for a passport will be required to hold an ID card until 1 January 2010. This is because of the compromise deal that was struck in order to get the Act passed. As mentioned earlier, the fact that an entry will still be made on the register arguably makes this a compromise of little consequence. Whatever the final timescale and rate of compulsion, the intention is that, eventually, all UK citizens and anyone else residing in the UK for over three months will have an ID Card.

A commonly used justification for the NIR and ID cards is the ‘nothing to hide, nothing to fear’ argument. As has been observed earlier, the fundamental misconception in this proposition is that privacy and criminality are synonymous. We all have information about ourselves that we would prefer kept private. If we did not, we would be quite happy to have our medical records freely

[120] http://news.bbc.co.uk/1/hi/uk/4794975.stm

[121] The LSE report is available at http://www.lse.ac.uk/collections/pressAndInformationOffice/PDF/IDreport.pdf

available to anyone who wished to see them. This does not make us criminals. 'Nothing to hide, nothing to fear' is invariably accompanied by the observation that many other countries have ID cards. Overlooking the differences that exist between the NIR and the schemes operating in other countries, this is a double-edged argument. Many countries with ID card schemes have experienced problems arising from excessive or discriminatory use of police and immigration officials' powers to demand identification from minority ethnic groups.

In order to counteract concerns over arbitrary and discriminatory demands for identification, the IDCA contains safeguards to protect against forced production of a card. Section 13 (3) specifically excludes the making of regulations which would require a person to carry an ID card at all times. Meanwhile Section 16 (2) creates a bar on any requirement that a person be required to produce a card. The combination of these two protections would appear to ensure that people will not be required to produce ID cards to the police or immigration services.

However, upon closer examination these safeguards are not as watertight as they originally appear. Section13 (3) might prevent regulations being passed requiring production. However, this only means that laws cannot be put into place expressly forcing people to produce cards. It does not prevent cards being used as a matter of course to establish identification. Section 16 might seem to provide some assistance as it does contain such a prohibition. However, there are a number of exemptions. In particular, Section 16 (3) removes the bar on production if a person is of a description of those who are subject to compulsory registration. It could be argued that what now constitutes compulsory registration might now be a moot point. For most of the Bill's progress, it contained a power for the Secretary of State to force compulsion by naming particular groups. The plan seemed to envisage initial designation of asylum seekers or refugees, then those from outside the European Economic Area. This would be followed by those from the EEA, and finally British citizens on a roll-out according to age [122]. However, this power was removed in order for the bill to receive Royal Assent. New legislation will be needed to force compulsion. What 'compulsion' means is debatable, as anyone who is required to register on the NIR when applying for their passport has no choice. They are effectively being compelled. In other words anyone registered this way might be considered 'compelled' for the purposes of Section 16 (3).

In any event it is clear the Government intends that everyone be eventually compelled to register. Designating passports will ensure that most people register but there will always be a few who do not have passports and who never will. The only way to ensure universal compulsion is by compelling registration.

When legislation is introduced allowing compulsion, roll-out is likely to then take place according to age as originally planned. This means that eventually everyone will be 'of a description of individuals subject to compulsory registration' and will fall into the exemption provided by Section 16 (3). In other words, no-one will be able to rely on the prohibition not to produce cards.

So does this mean that production of ID cards might be required as a matter of course? The Government might maintain that this will not happen, but the application of standard policing powers suggests it might well.

---

[122] There were some problems with this, in particular how Irish citizens would be treated, but this appeared to be the basic plan.

The reality of policing makes stopping people to establish their identity a regular occurrence. Section 24 of The Police and Criminal Evidence Act 1984 allows for arrest without warrant for a number of reasons including enabling the name of the person in question to be ascertained. This means that ID cards are likely effectively to become the means by which identity is established. This will particularly be the case with the use of broad powers of stop and search without suspicion, available throughout London on rolling authorisation since 2002 under Section 44 of the Terrorism Act 2000.

Coupled to this is a concern that identity cards will be used as a means of internal immigration control. In September 2004, *The Guardian* newspaper ran a story saying that police and immigration officials had carried out random swoops on public transport [123]. The then immigration minister, Des Browne, said that officials could legitimately question people to determine their immigration status where there is a reasonable suspicion that a person is an immigration offender. Given that Clause 1 (5) of the Bill allows 'current residential' status as a registrable fact, it is a significant concern that once the scheme has moved to compulsion, members of minority ethnic communities will be required to produce their identity card on a regular basis by police and immigration officials. Once compulsion has been fully rolled out and the scheme settled in, there is also the possibility that not carrying a card, although perfectly legitimate, might be viewed as something that is in itself suspicious.

## Access to the Register

The privacy implications of any database are dependent on who can have access to it. There is a huge difference between information retention and information dissemination. People are not generally concerned by the holding of extremely sensitive personal data about ourselves if we are relatively confident that that information will not be shared. Medical records contain information that is certainly more 'private' than the information that will be held on the NIR. However, people do not generally take issue with this as they do not expect that our medical information will be accessible by a range of public and private bodies [124].

The Act creates a wide ranging regime allowing access to the register without consent [125] to named public bodies and agencies. It also allows information to be provided to private sector bodies with a person's consent [126] in order to assist with verification. This will enable information to be passed to private bodies such as banks in order to verify identity.

Powers to pass information without consent are largely restricted to public bodies (although information can be passed to anyone for the purposes of crime detection and prevention). The Act sets out a list of bodies that can be given access to the register. This contains all those bodies that might be expected: the Security Services, GCHQ, various policing bodies, the Commissioners of Customs and Excise. The police and customs bodies do have some restriction on their ability to access the register in that it must be for a purpose linked to national security, crime and so on. The

[123] http://www.guardian.co.uk/immigration/story/0,,1422817,00.html

[124] NHS Connecting for Health, responsible for the planned centralisation of patient records, has been at pains to emphasise the restrictions to access intended to ensure that no-one can access records without good reason.

[125] Sections 17-21

[126] Section 12

security services and some specialist police agencies such as the Serious Organised Crime Agency (SOCA) have effectively unfettered access. They are also able to access the 'audit trail' of the register.

The 'audit trail' creates some particularly interesting privacy implications for the scheme. Paragraph 9 of Schedule 1 to the IDCA goes far beyond the basic name, address, nationality and so on to be recorded in the register. It allows for a record to be made of every occasion where information in the register is provided to anyone, details of the person to whom the information has been given and 'other particulars' relating to each occasion this is done. As the register is rolled out, a growing number of both public and private sector bodies will provide an interface to the NIR. This means that a detailed record of everyone's movements, what services they have accessed at what time, and so on, will be collated. This will create an imprint of our existence going way beyond that currently created. Some agencies will have unlimited access to it without consent and without the need to justify access.

While the framework set up by the Bill is broad, it has considerable scope for extension. All powers of access are subject to extension by order of the Secretary of State. It does seem inevitable that many agencies that might be considered suitable to gain access to the register will eventually be granted access. This is not some unfounded 'Big Brother' prediction. It has logic and a precedent.

The logic derives from the fact that once a system is in place it is sensible to seek as many uses for it as possible. If there is any justification for a particular public or private body to be given access then it is unlikely to be rejected. No government would like to run the risk of allegations that a crime or terrorist attack could have been prevented if only access to the register had been given to a particular body. That would be political disaster. Far preferable would be the prospect of a few allegations of insufficient attention being paid to privacy.

The precedent comes from RIPA. As discussed earlier, RIPA sets out the powers and abilities of public bodies to undertake differing levels of targeted surveillance such as intercepting communications, using undercover operatives and obtaining communications traffic. The scheme as set up in the legislation is structurally similar to the IDCA. The legislation creates the scope of powers and allows regulations to list those that can use them. Once RIPA was in operation, the Home Office published regulations in 2003 that would have allowed an unprecedented range of 'public bodies' access to communications data such as records of emails and telephone or mobile phone conversations. The regulations, dubbed in the press 'the Snooper's Charter', allowed all local authorities as well as such diverse bodies as the Food Standards Agency and New Forest District Council powers to access data. Once *The Guardian* newspaper had run the story there was a surprisingly high level of public concern resulting in the Government promising to look again at its plans. This was notable for two reasons. First, the backlash against the plans demonstrated that people could be highly engaged by the prospect of intrusion from sources other than police and security services. It appeared that people were much less trusting of their local authority than of MI5. Second, this was, and remains, one of the few instances where secondary legislation by way of regulation has not been passed as a matter of course. In fact, the most surprising thing about the Snooper's Charter was that any attention was paid to it at all. When the revised and reduced list of public bodies was published it passed though parliament almost unnoticed. It is likely that any set of regulations passed under the IDCA will also eventually be passed with little attention being paid to their content.

## Privacy Safeguards

Despite the very real privacy concerns surrounding the creation of the NIR it is not an information free-for-all. As well as the limitations on information that will be held and who can have access to it, there are other safeguards. Some of these were introduced by amendments laid down by concerned parliamentarians as the Bill(s) passed through the Houses. Others were introduced by the Government in order to ease progress. None of these changes have had any substantive impact upon the IDCA, their cumulative total effect being described by Liberty as 'rearranging the deckchairs on the Titanic'. They do however, provide some protection against improper use, abuse and also provide some oversight of the scheme. Examples of safeguards include the restriction mentioned earlier that identifying numbers recorded on the register could not allow for the recording of sensitive personal data defined by S. 2 of the DPA. The penalties for improper disclosure of information from the register were also made more robust during progress through Parliament.

The IDCA does place obligations upon those entered on the register to pass on any information about changes. This does provide some degree of quality control. However what is lacking is much scope for individual self verification of entries on the NIR. Greater scope for individuals to check, and if necessary correct, their entry would have provided a much more effective way of maintaining the accuracy of the register. Any database is only as effective as the quality of the data it contains. The scope for problems caused by dissemination of incorrect information has always undermined the effectiveness of databases. The lack of information vetting was a concern throughout the progress of the IDCA and remains a real anxiety.

Another concern was the potential for abuse of the NIR. There will be many people who will have potential access to the register. Consequently there will also be the opportunity to pass on information to those who are not entitled to it or to tamper with the register. These concerns are directly addressed by the Act, which creates specific criminal offences of 'unauthorised disclosure of information' and 'tampering with the register'. These offences should go some way to ensuring that at least the potential for abuse is lessened.

Oversight of the scheme is the responsibility of the new office of National Identity Scheme Commissioner. The role, although impressive sounding, is not quite the powerful independent regulator many were hoping to see. The role was strengthened considerably subsequent to publication of the first Bill, but is still somewhat limited [127]. The Commissioner will review arrangements being made under the powers created by the Act, the arrangements made for obtaining information and the uses to which ID cards are put. What s/he will not do is review any other part of the Act or report directly to parliament. The commissioner will provide an annual report to the Secretary of State, who will then be able to remove any parts which s/he feels might be prejudicial to national security or to crime detection or prevention before parliament sees it.

There are a number of functions the Commissioner is specifically barred from. S/he cannot comment on a range of listed topics such as any of the extensive civil and criminal penalty regime created by the Act, about the way regulations are exercised, or about the provision of information to the security services. All in all, the statutory powers of the Commissioner fare poorly when compared with that of other regulatory Commissioners such as the Information Commissioner.

[127] The Commissioner's role is set out in Sections 22 & 23 of the Act

## The future

What will happen? Much of what has been said in this chapter is supposition. It has been necessary to focus on the legislation as there is no ID card scheme in operation and the NIR is (presumably) still on the drawing board. The mass informational database which will have privacy implications for each of us, going beyond anything else that has occurred since the last scheme was abolished in the 1950s, does not yet exist.

So will it ever? At the time of writing it is difficult to say. The UK Borders Bill was published early in 2007. It sets out the legislative framework for a Biometric Identification Document. This will be issued to all non EEA residents in the UK and is intended to be the first part of the roll out towards the full ID card programme. However, this too is still merely at the legislative stage.

The new Prime Minister, Gordon Brown, has publicly stated his continuing support for the scheme, making particular reference to its relevance to national security. The extent of his support is still difficult to gauge. When the Bill was before Parliament there were rumours that he had private reservations about the Scheme and he has certainly never been as vocal a supporter of ID cards as his predecessor.

The two main opposition parties have said they will make manifesto commitments to scrapping ID cards if they gain power. There remains the possibility that, the whole scheme may still be unceremoniously scrapped. The national media publishes stories with what must be galling regularity for the Home Office about the latest technical glitch to the ID scheme[128]. Rising costs are increasingly an issue and the government was accused in May 2007 of attempting to bury bad news about increasing expenses behind the news of Tony Blair's resignation[129].

With so many uncertainties it is difficult to make confident predictions. The tendering process itself looks to be problematic. The size and generalised nature of the database has made it difficult for the Home Office to be specific about requirements. In December 2006 the Government announced that it had abandoned plans for a single database to run the scheme. Instead of a single multi-billion pound system, information will be held on three existing, separate databases. The information is now to be spread across three existing IT systems, including the Department of Work and Pensions' (DWP) Customer Information Service, which holds national insurance records[130].

Originally the proposal was to rely on identification through biometric information. It appears that there has been a growing awareness that this is simply unrealistic, making it possible that the NIR is going to downgrade from biometrics and associated data centres to a chip-and-pin system. This has created further problems as there are significant concerns about the security issues associated with chip-and-pin. There is also the possibility that deviation from the original scheme might require amendment to the IDCA. Furthermore, removal of the biometric data from the ID card programme would remove one of the central justifications for the scheme to be introduced. The Government has long maintained that Europe-wide moves towards biometric passports have legitimised both the principle and the cost of a biometric identifier.

---

[128] See for example http://news.bbc.co.uk/1/hi/uk_politics/5173706.stm and other sources too numerous to list.

[129] http://www.dailymail.co.uk/pages/live/articles/news/news.html?in_article_id=453866&in_page_id=1770

[130] http://news.bbc.co.uk/1/hi/uk_politics/6192419.stm

The initial scope of the scheme is also difficult to predict. The organisation No2ID has estimated there will be approximately 265 public and 44, 000 private agencies expected to make use of the NIR. Again this is likely to present practical difficulties. For example organisations will have to deal with situations in which the individuals about whom they are concerned are given yet another number. This will have massive internal resource implications for a huge number of bodies. The ancillary costs to public bodies have not been factored into cost analysis. Again it is difficult to anticipate the cost to local authorities of implementing the NIR and ID card systems. It is likely to run into millions per authority. Presumably this will have to be raised through council tax raises or through cuts to other services.

If all the political, cost and myriad other problems are overcome, the scheme has the potential for massive privacy implication going beyond what the IDCA itself envisages. The NIR has the potential to be the hub for all public sector databases. Early on during debate on the ID card Bill, there were plans to link it to the (then) proposed Citizen Information Project (CIP) data spine. This would have included information about a person from a record of their birth throughout life until a final record of their death. The CIP has now been abandoned, but there is potential to incorporate something similar in the NIR. Inherent in plans for the NIR is the creation of a single unique identifying number.

The concept of a "meta-database" is created when this number is used to link through to other databases. Without firm proposals, it is not possible to consider the implications of this in any detail. There is also a danger that predicting what might happen in the future might give rise to allegations of paranoia. However, given the history of the CIP and other indications of the government's attitudes to information sharing, it is not too much of a leap of logic to predict what might occur over the next few years.

As time progresses, it will become increasingly common for people to use a card that will propagate the key to their personal information. Individuals will do this across a range of databases as they use the card, and the government will then be able to access a wide range of information by following the trails of legal and correct use. Individuals will, at most, only see part of the NIR trail; they will not be able to see and trace other links. However, the police and other security and enforcement agencies will be able to track links across databases. For example, a list of people is generated, and then searches made against all of them for other links which might be relevant to a criminal investigation, such as visits made to banks or to hospitals, for example. What could eventually occur is the mass holding of informational data which can then be accessed in order to ascertain potential links to, for example, criminal activity.

This goes way beyond the sort of legitimate intelligence-targeted surveillance currently used to investigate crime. It is far closer to the sort of profiling techniques sometimes alluded to, and then dismissed, by government ministers following emergencies. As mentioned earlier, following the July 2005 attacks and the alleged plot to blow up aircraft in August 2006, suggestions of profiling that were essentially based on racial characteristics were made about tube and air passengers respectively.

It would not take significant amendment to the existing Act to allow far greater degrees of profiling to take place than were considered by parliament. As has been considered earlier, the ability for significant data auditing has already been incorporated into the Act. Linked databases with increased data would allow for wholesale and detailed extension of this audit trail.

All this may never happen. The NIR may never get off the ground. Whether it does or not, as a society we still experience levels of mass informational surveillance simply unimaginable when the Labour Government came to power.

## The Children Index

The Children Index is the name given to the database created under the Children Act 2004. The genesis for the database was Lord Laming's report into the death of Victoria Climbié in January 2003[131]. This was followed in September 2003 by a Green Paper '*Every Child Matters*'[132]. Much of the content of Lord Laming's report and Every Child Matters concerned the need for a new body safeguarding the interest of children and other structural changes. However recommendation 17 of Lord Laming's report, which attracted limited interest at the time, suggested 'The Government… actively explore the benefit to children of setting up and operating a national children's database on all children under the age of 16'[133]. This idea was enthusiastically taken up in Every Child Matters which devoted most of a chapter to the proposal. Every Child Matters envisaged an information hub containing a child's 'name, address and date of birth; school attended or if excluded or refused access; GP; a flag stating whether the child was known to agencies such as education welfare, social services, police and Youth Offending Teams (YOTs), and if so, the contact details of the professional dealing with the case; where a child is known to more than one specialist agency, the lead professional who takes overall responsibility for the case'[134]. Twelve separate bodies were identified as needing access to this information[135]. It is apparent that in its early stage the information contained on the children register and the bodies entitled to access this information went well beyond what was later proposed in the Children index.

It should be emphasised that there was little dispute over the policy driver behind the creation of the index. The idea that appropriate information sharing could and should take place between appropriate bodies with issues of concern being flagged for action was and remains absolutely non-contentious. The concerns that were raised focused on the necessity and potential counter-productivity of the plans and the sheer volume of data that was to be retained.

At the heart of these was the implicit suggestion that the previous law was insufficient. The existing relevant statutory express provisions allowing information had been contained in the Children's Act 1989 and The DPA. The DPA for example explicitly allowed information sharing in order to protect the vital interests of the person about who the information is held or to assist with the prevention and detection of crime. It was misleading to imply that information sharing was prohibited before the Children Act. What Victoria Climbié's case did demonstrate was a serious lack of understanding, resource and training by the care professionals involved. The creation of a database, and information sharing *per se*, cannot by themselves address these problems.

When the Children Bill was published in early 2004 there was widespread concern about the potentially counterproductive impact that mass data collection and dissemination could have. Even major children's charities such as the NSPCC, which might not have been expected to comment on 'privacy' issues such as information sharing expressed concern saying '*Local authorities could end*

---

[131] http://www.victoria-climbie-inquiry.org.uk/finreport/finreport.htm

[132] http://www.everychildmatters.gov.uk/_files/EBE7EEAC90382663E0D5BBF24C99A7AC.pdf

[133] Ibid 26 at page 373

[134] Ibid 27 at paragraph 4.3

[135] Identified at paragraph 4.6 as Children's Fund Services; Sure Start; Voluntary Sector; Primary Health; Child and Adolescent Mental Health Services; Social Care; YOT; Police; Housing; Education Welfare; Education Psychology; Education Schools.

*up with complex databases which contain too much highly-sensitive information that would be difficult to interpret out of context. The cost of this, both in human and financial terms, could be very high*'. In effect critics were warning of the worst of all possible worlds. A database with excessive scope for information retention could result in information giving rise to a 'cause for concern' [136] being recorded to such an extent that indicators of a child genuinely being at risk might be missed by not 'seeing the woods for the trees'. It is easy to see how a social worker or other person inputting data would be tempted to always err on the side of caution when deciding what information to enter on the index so as to avoid culpability in the future.

On the other hand, the mass retention and dissemination of data created the prospect of privacy intrusion to children and their families. The information hub imagined in the white paper would have allowed a multitude of agencies access to information not only about children and their families. If for example, the mother of a child suffered from post-natal depression, that might be considered information that was a 'cause for concern' relevant to a number of agencies even though it was private and sensitive medical data.

The Children Bill remained relatively unchanged during its progress through Parliament and became the Children Act 2004. The debates in Parliament were distinct from those on the ID card bill in that there was little expression of principled opposition to the concept of a database of children at risk. Concerns centred on the potential for familial intrusion without a corresponding child protection benefit. These were exacerbated by the fact that entry onto the children's index was not to be limited to children who were considered at risk. All children will be included. This raises an interesting proportionality issue in that the privacy concerns might have been considered less of an issue if the case for child protection had been more widely accepted. However, when the Bill was passing through Parliament both privacy lobbyists and those primarily interested in child protection seemed to agree that the Bill served neither cause particularly well. As the Children's Legal Centre, an organisation concerned with children's privacy and wider children's rights issues said, '*Although the underlying intention is entirely positive, the operation of such a system raises issues of human rights and data protection which must also be considered when deciding where the best interests of the child lie*' [137].

It appears that some of the concerns expressed during passage of the Bill were at least partially taken on board by the Government. As with much privacy legislation the detail on exactly who would be able to access what information was not written onto the face of the Bill but reserved for a later date to be published in regulations. These regulations went out to public consultation in late 2006 and demonstrated that there had been some attention paid to the potential for mass informational overload. For example details of 'sensitive services' such as mental health, sexual health or substance abuse treatment would not be entered onto the register (although the fact that a sensitive service was being received would be). Anyone with access to the register would need a Criminal Records Bureau check and would need to have received proper training. The regulations also recognised that consent was an important and relevant issue and attempted to incorporate a consent requirement for certain types of informational disclosure.

---

[136] Section 12 (4) (g) of the Children Act 2004 allows the recording of '*information as to the existence of any cause for concern in relation to him*'

[137] http://www.childrenslegalcentre.com/shared_asp_files/uploadedfiles/%7BDFA9D7E3-8287-4621-93F4-89F386DAB618%7D_Information%20Sharing%20Databases.pdf

Notwithstanding such improvements, the scope of those who might access the register remained extremely broad. Similarly, arrangement of and provision for training of those to have access to the register remained essentially a matter of local interpretation. While attempts had been made to address the issue of consent this remains a difficult area particularly in determining what constitutes proper, informed and non-coercive consent for a child. Giving multiple agencies access to the register over a period of time also muddies the waters of what constitutes consent.

At the time of writing the regulations have not been published in Parliament. It is likely however that they will be similar in form to the draft put out for consultation. As the voting procedure for regulations only allows for them to stand or fall as a whole it is extremely unlikely that they will not pass through in the same form as published.

The Children Index, if used properly, has the potential to be a valuable resource for ensuring child protection. However, it also has the capability to have a detrimental child protection impact though over-provision of information. It could undermine the privacy of children and families. It might have health treatment implications as a result of children not seeking health advice or medical care for fear of that information being passed on. It could prove an ineffective and burdensome tool for those entering and accessing the index if they do not have adequate training, guidance and resources.

The Government does seem to be aware of the potential risks the Index presents. This is reflected in the need for guidance to be issued by those using the register. The importance of this cannot be stressed enough. However the issuing of guidance is one thing, its effective implementation is another. The experience of the Bichard Inquiry into the Soham murders showed that guidance can remain unimplemented and misinterpreted unless properly introduced and carried though. During the Bichard Inquiry it became apparent that guidance on retention and dissemination of 'soft' information [138] agreed between the Information Commissioners Office (ICO) and the Association of Chief Police Officers (ACPO) was rarely relied on. This was due to a general lack of awareness of the guidance and vague drafting that proved difficult to interpret.

If there is a tendency for legislation and regulation to be drafted in broad terms then this is effectively delegating down the operational interpretation. Guidance has always been part and parcel of interpretation of legislation as laws can only be expected to set out a framework. However, it can be argued that this form of delegation has increased over the last few years with secondary legislation and guidance increasingly being relied on as the means to put flesh on the bones. This will increase the relevance of statutory bodies such as the ICO in providing proper data protection and privacy-compliant operation. There will be a huge range of bodies accessing the Children Index. As with any employment sector, staff turnover will mean that training in guidance will need to be regularly applied to ensure that it does not fall into disuse. Bodies or agencies able to add to or access the register will need to have designated officials capable of dealing with complex issues of consent. Strategic national oversight will be necessary to ensure that different local agencies do not have differing interpretations of guidance. All these factors will require time and resource but will be essential to ensure that national rollout of potentially invasive and counterproductive systems operate in as effective a manner as possible.

[138] Soft information involves allegations, suspicions and criminal proceedings against individuals which do not result in criminal convictions.

If we are moving into a society where mass information retention and sharing is an increasingly integral part of public sector operation, then there are corresponding obligations placed on the state to ensure that they work effectively and efficiently. There is no avoiding the cost and resource impact of ensuring that the ICO and other agencies are able effectively to 'police' privacy. These costs should be factored into any cost-benefit analysis at an early, if necessary pre-legislative, stage. There are societal benefits that can arise from proportionate mass informational information sharing for legitimate purposes. However without a supportive framework ensuring appropriate exercise and application of information sharing powers, the bad might outweigh the good.

# 6. The National DNA Database

In an answer to a parliamentary question from the Conservative MP Mark Pritchard on 20 June 2007, the Home office Minster Joan Ryan confirmed that as of 10 June 2007 there were an estimated 3,976,090 people who had samples retained on the National DNA database (the 'Database' or the 'NDNAD') [139]. This equates to 5.2 per cent of the population. The UK's NDNAD holds five times the percentage of the population as the next largest (Austria) and is ten times the proportion of the USA's database.

In recent years the NDNAD has increasingly become an issue of privacy interest. The use of DNA as a tool in criminal investigation dates from the late 80s. The database itself came into existence in 1995. At first only samples from those convicted of certain offences were retained on the database. Since then legislative changes have greatly increased the scope of entry onto the register. As a consequence, anyone now arrested for a recordable offence [140] can have their DNA taken and permanently retained. This has resulted in ever-increasing numbers of people who have never been convicted, cautioned or even charged with an offence being entered on the register. Five per cent of the UK's population are now in the register. This is five times the proportion of any other country. The growth of the database has made conflict with privacy principles inevitable.

The NDAD undoubtedly raises profound legal and ethical concerns. Of particular concern is the permanent retention of the DNA of everyone who is arrested and the severe over-representation of young black males in the samples currently contained in the Database. Consequential to this are the potential uses that DNA information might be used for. Such issues have, however, received surprisingly little political attention. The Database was established without any Parliamentary debate and the political discourse has since been dominated by Government claims about the utility of the NDNAD in tackling crime.

Debate over ID cards and CCTV has remained consistently high on the public agenda. It has also been relatively balanced in that proponents and critics will usually be debating the same points. A

[139] Parliamentary Question 114068 20 June 2007.

[140] Recordable offences are generally those which can result in a custodial sentence.

debate through the media or in Parliament over the desirability or otherwise of the National Identity Register will focus on roughly the same issues; effectiveness; cost; societal impact and so on. This has not happened in debate over the DNA database. Media interest in particular has tended to arise following the conviction of a person for an offence committed years ago thanks to advances in DNA technology. In this context it is extremely difficult to debate the privacy and equality implications of the Database when the subtext is the rhetorically powerful but unrealistic implication of movement towards a risk-free society or one in which all criminals are brought to justice thanks to the NDNAD.

There is no debate over the desirability of a NDNAD. It has proved a valuable crime detection tool. Part of the problem that those who have expressed concerns about extension have experienced is the distinction between justification *per se* and proportionality. If the DNA database can help solve crime there is a crude logic to the argument that the further it is extended, the more crime will be solved. Liberty's starting point has always been that a person's DNA is private information and that the collection, retention and use of that information engage their right to privacy. This is because DNA is information about a person's genetic make-up. As a consequence this kind of information belongs, *prima facie*, to the individual concerned and not to the state. As La Forest J explained in *R v. Dyment* "This notion of privacy derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit" [141].

This does not, of course, mean that it will never be justified for the state to take, retain and use someone's personal information, even their DNA. Instead, it means that the state should be required to justify such actions. First, is there a legitimate reason for the intrusion of privacy that the NDNAD constitutes? Secondly, could that legitimate aim be achieved in a way which does not intrude into a person's privacy or could do so less? As citizens we are entitled to ask these questions and trust that responsible, democratic and accountable Governments should not shy away from providing us with the answers. Only then can we make up our own minds about the validity of these arguments. A culture of justification is, we believe, integral to good policy making, Government accountability and an engaged citizenship.

These questions of proportionality and legitimate purpose are the same as the courts are required to ask under the Human Rights Act 1998 when deciding whether a state action or law, engaging Article 8 of the European Convention on Human Rights (right to respect for private and family life) is justified [142]. The domestic courts have accepted that the taking and use of DNA engages Article 8 and have therefore required a degree of justification for such actions from the Government. They have not, however, conducted a very rigorous assessment of the "law-enforcement" justifications they have been given. The courts' approach has been even worse as regards the indefinite retention of DNA. They have not even considered this to fall within the remit of Article 8 and, therefore, required no justification from the Government [143]. The majority decision in *Marper* (where this determination was made) was a serious blow to those who hoped that at least the concept of privacy protection would be extended in relation to DNA. The European Court of Human Rights (ECtHR) has recently declared Marper admissible [144] so there is the prospect that there might presently be a determination that the retention of DNA at least engages Article 8.

---

[141] (1988) 45 CCC (3d) 244, at 255-256).

[142] Article 8(2).

[143] *R (S and Marper) v Chief Constable of S. Yorks & Home Secretary*, [2004] UKHL 39.

[144] Application 30562/04 and 30566/04.

While disappointing, the courts' approach is, perhaps, unsurprising. Government schemes that impact on privacy (like the Database and ID Cards) often involve relatively low-level and less tangible infringements of an individual litigant in human rights. It is only by aggregating the impact of these schemes across the millions of people they affect that the real extent of the privacy infringement becomes clear. When an individual's case is brought before a court, the judge does not have the institutional capacity to assess whether the benefits of the scheme really justify the millions of low-level rights violations the scheme involves. In fact, s/he is presented with and asked to adjudicate only on the single low-level violation brought before him/her. When this single privacy infringement is balanced against the grand and compelling claims of "accurate and efficient law enforcement" presented as a justification by the Government, it is not surprising that, more often than not, the courts decide in favour of the Government[145]. This is why extra-judicial mechanisms are so important in protecting our privacy rights against sweeping Government initiatives like the NDNAD and ID Cards.

It seems that Parliamentarians are increasingly aware of the impact of these schemes. While the issue does not seem to have become a significant party issue yet individual MPs have raised DNA as a campaigning issue. The Conservative MP for Welwyn Hatfield Grant Shapps is running a campaign to try and remove all those under 16 who have had their DNA retained despite not being cautioned or convicted of an offence. Similarly the Liberal Democrat MP Lynne Featherstone has consistently written about, asked parliamentary questions over and campaigned on DNA retention. As the NDNAD continues to roll out and retention becomes an issue concerning millions it is likely that politicians will increasingly acknowledge DNA as an issue.

## Sampling Powers

There are a range of ethical issues raised by the taking of DNA samples and fingerprints. To begin with there is an initial distinction to be made between the indefinite retention of DNA and the initial taking of this bioinformation. There are many legitimate reasons why the police may need to take a suspect's fingerprints or DNA during the course of a criminal investigation. This information could, for example, help the police to determine whether a suspect was at a crime scene and/or to confirm a person's identity. During the course of a criminal investigation there may also be a good reason to request the DNA and/or fingerprints of a person who is not suspected of committing any crimes (i.e. a witness or victim). This could for example help the police to eliminate non-suspect bioinformation found at a crime scene. If a justification like these exists, it is unlikely that the taking of DNA samples or fingerprints for the purposes and duration of a particular criminal investigation would raise particular privacy concerns.

Some of the other ethical issues which could arise from the taking of bioinformation in the context of a criminal investigation are also worth mentioning:

- The potential for taking samples in a manner or at a time that is likely to cause unnecessary distress or inconvenience to the person concerned. It would be more invasive for example to wake a suspect in police custody on several occasions during the course of a night to take samples which could have been taken upon arrival at the station.

[145] In terms of human rights litigation, cases like that of *S and Marper* are at the other end of the spectrum from torture cases which usually involve a very severe rights violation which affect very few people and, in which, adjudication of individual cases is particularly well-placed to protect rights.

- The need to adopt the least intrusive method of taking bioinformation. If a mouth swab would suffice there is arguably no justification for the taking of a blood sample.
- The need for particular sensitivity when taking DNA from victims and other vulnerable people.
- The need for a clear explanation of the reason and legal power being used to take the sample.

Guidance on the applicable rules on retention and use of the sample need to ensure that these issues are considered. At present Code D of the Codes of Practice issued under the Police and Criminal Evidence Act 1984 covers the regime allowing for the taking of DNA samples.

## Retention of Samples

The Criminal Justice Act 2003 provides for the retention of DNA samples and profiles regardless of whether a person is prosecuted or cleared of an offence. It means that even if a person is never charged with an offence for which s/he was arrested his/her DNA will be retained on the Database indefinitely. A person who has had their DNA retained can apply to the police to destroy the sample but the police's discretion to do so is not frequently exercised. This wide ranging power of retention is the reason the UK holds a far greater proportion of its population on its database than any other country. Powers of retention may soon be extended further so that arrest for any offence (rather than just recordable offences) will allow the taking of a sample. This is what seems to be implied in the Home Office consultation 'Modernising Police Powers: Review of the police and Criminal Evidence Act (PACE) 1984' which states, "*The absence of the ability to take fingerprints etc in relation to all offences may be considered to undermine the value and purpose of having the ability to confirm or disprove identification and, importantly, to make checks on a searchable database aimed at detecting existing and future offending and protecting the public. There have been notable successes particularly through the use of the DNA database in bringing offenders to justice*"[146]. The consultation does not specifically state the NDNAD when applying biometric retention for all arrests, using the slightly vague 'fingerprints etc'. However the reference to the DNA database at the end of the paragraph is a strong indication of what 'fingerprints etc' might entail. If the power to take and retain DNA is expanded in this way it will mean that offences such as dropping litter might be included[147]. Should this occur, a wholesale expansion of the DNA database is likely.

As described earlier, justification for retention is usually described in terms of a vague wider societal benefit through crime detection accruing from the taking of DNA. However many of the arguments in favour of the retention of DNA profiles of everyone arrested do not stand up to close scrutiny.

There must be a rationale justifying the DNA retention of those who have been arrested but not charged or cautioned of an offence as opposed to retention from a random sample of the population. This rationale must be that retention from these people will result in an overall improvement in DNA use for the detection of crime as compared with random sampling. However, there does not seem to be any evidence to support this assumption. This was accepted by the Government on 9th October 2006, when Home Office Minister Joan Ryan stated "As far as we are aware, there is no definitive data available on whether persons arrested but not proceeded against are more likely to offend than the population at large"[148]. As a consequence there does not seem to be any basis for distinguishing

[146] http://www.homeoffice.gov.uk/documents/cons-2007-pace-review?view=Binary at paragraph 3.33.

[147] Dropping litter is an offence under S.87 Environmental Protection Act 1990.

[148] 8th October 2006, HC Deb, Col 491W.

these people from the population as a whole. The current approach therefore seems to discriminate against those sampled on the basis of arrest. Without evidential backing it appears that the policy basis for permanent retention of those arrested can be little more than 'people who are arrested are probably criminal even if nothing can be proven in this case'. Given the disproportionately high number of Afro-Caribbean males on the NDNAD this is a worrying conclusion.

The assertions put forward by police and Government as to the number of 'matches' made to the DNA profiles of unconvicted persons are highly misleading since (a) 'matches' only result in convictions in a small proportion of cases and no conviction information is given; (b) no information is given as to whether those persons were already suspects or would have been otherwise identified through traditional policing methods; and (c) the figures are probably inflated by the inclusion of a high (but necessarily diminishing) proportion of 'cold cases' relating to crimes committed before the police had today's capacity to use DNA in crime detection.

In addition, there is no evidence that the detection of crime is improved by increasing the size of the Database. This is illustrated by the fact that, although there has been a massive extension of the NDNAD over the last three to four years, the rate of crime detection using the Database has stayed at about 0.35% of all recorded crime. If extending the size of the NDNAD had been successful one would expect this proportion to have increased. One limiting factor is that the usefulness of the Database is driven by the ability to obtain DNA from the crime scene. In many cases DNA is not available. Regardless of advances in DNA technology it remains the case that DNA is relevant only in a limited number of cases. Primarily these will be investigations involving sexual assault or violence. These represent a small proportion of overall crime[149]. In many allegations involving sexual assault, consent rather than identity will be the defining issue. Similarly, evidential issues around violent crime will often be based on self defence or degree of involvement rather than establishing actual presence. Overall the importance of DNA attaches to a very small number of cases. However, its importance as an evidential tool is dramatically enhanced in the public consciousness when DNA provides the 'magic bullet' allowing an historic crime to be solved. The fact that these crimes tend to be of an extremely serious and dramatic nature tends to mask the relatively small impact DNA has on the criminal justice system as a whole.

The retention of DNA from individual demographic groupings raises particular issues over the retention of children's DNA on the Database. An estimated 50,000 of those whose DNA has been taken and retained on the database are children. There are also a disproportionate number of black men on the NDNAD. As stated in the introduction to surveillance almost 40% of black men have their DNA profile on the database compared with 13% of Asian men and 9% of white men[150]. Within the Metropolitan Police area, 51% of the innocent (uncharged/unconvicted) people whose DNA is held on the Database are of black or other minority ethnic origin.

The NDNAD does not exist in a vacuum and its privacy implications are arguably exacerbated by its connection with other sources of information and other Government databases:

---

[149] According the British Crime Survey Statistics for 2005-2006 there were 40,300 Serious Violent Crimes Against the person (including sexual assault and firearms offences) out of a total of 5,556500 total recorded crimes. This is about 0.7% of the total.

[150] See footnote 12 above.

- Private companies, for an annual fee, retain the samples from which the data contained in the NDNAD are derived. These samples contain vast amounts of genetic information, including health-related information. There is nothing to prevent these companies using samples to develop mini databases of DNA records.
- The Database is also connected to the Police National Computer. This could exacerbate privacy implications because connections can be drawn between sets of personal data. Similarly PNC records are now retained indefinitely as a result of the link to the Database, whereas before they would have been weeded out after a short period of time. Furthermore, information contained on the PNC is visible to a wider range of non-policing bodies. In short, the effect of the NDNAD is not limited to that database but has a wider impact on other police records.
- It is possible in the future that connections will be made between the National Identity Register and the Database. A recent Home Office document on the NIR explains that "it will have links with other Government systems to share identity data" and even suggests that the biometric data element of the NIR will, in fact, be stored on "existing biometric systems"[151]. If the bioinformation in the NDNAD were to form part of the NIR, this would represent a significant extension of the stated law-enforcement purpose of the Database. Linking the NIR with other biometric databases is clearly already part of Government thinking. The former Prime Minister Tony Blair made this clear when sending an email to the 27, 000 signatories to an anti ID card petition on the Number 10 website. In it he said "I believe that the National Identity Register will help police bring those guilty of serious crimes to justice. They will be able, for example, to compare the fingerprints found at the scene of some 900,000 unsolved crimes against the information held on the register."

## Voluntary DNA samples

DNA is occasionally provided voluntarily. This might occur if a victim of crime provides their DNA for elimination purposes during the course of a criminal investigation. Samples might also be volunteered to the police in response to requests for people in a geographical location to rule themselves out of a crime investigation. At present over 12,000 volunteer samples are contained in the Database. The samples that are retained may be used in the future in the same way as samples taken from convicted criminals. A person who has volunteered for their DNA to be put in the Database has no right to have this bioinformation removed. This can prove to be problematic both in principle and practice. If a person's consent is needed to take a DNA sample then it might be expected that they are able withdraw that consent and consequently to require their sample to be removed. This might raise practical concerns if people are aware that any bioinformation they voluntarily provide could be retained for future use, they might be less inclined to co-operate. In the long run it might be that a failure automatically to destroy any sample provided to the police might hinder investigations.

## Uses of DNA samples

Some of the uses of DNA potentially raise ethical issues. The police are currently in favour of the recovery of physical information on an individual (from crime scene DNA where there is no match to

[151] *Strategic Action Plan for the National Identity Scheme: Safeguarding your Identity*, Home Office, December 2006, pages 7 and 11.

an NDNAD entry) in order to obtain information about the appearance of a perpetrator. This could represent a move into a class of genetic marker of considerable importance to an individual. Such markers could, for example, carry information on disease liability (for instance, a gene involved in facial appearance could well carry variants that might cause congenital malformation in a carrier's offspring). This information might give the police access to inappropriate medical and ethnic information.

The technique known as "familial searching" could also lead to privacy concerns. Familial searching is the process whereby the NDNAD is used to assemble a list of possible relatives of the owner of a particular DNA sample. The list of possible relatives is obtained by identifying individuals whose Database profiles show a statistically significant similarity to a profile from a crime scene sample but which do not exactly match the sample profile. Each familial search throws up 50-150 possible relatives and about 80 searches are being undertaken each year. The consequence of this is that many innocent individuals might be brought into a criminal investigation on the basis of the familial match. Familial searching could also unwittingly reveal to the police information about private personal relationships. A genetic link between individuals could be previously unknown to one or both parties and police investigations may make this information known for the first time. This is a relevant issue given that an estimated 1 in 30 people in the UK are mistaken as to the true identity of their biological father. Familial searching also risks disclosure by police of the fact that an individual has been arrested to their family members.

Twenty or so research projects using the NDNAD have been allowed since 2000. However, the procedure for approving research uses of the NDNAD lacks transparency. It might prove to be in the public interest to provide greater detail about the nature of these projects. This could include an ethical review of applications to use the database and the associated samples for research purposes. Without tight regulation, there is no reason why a great variety of tests could not be conducted on many of the millions of genetic markers in human DNA to reveal highly sensitive information about ethnic origin, physical appearance and disease liability.

# 7. Privacy and the Media

## Introduction

This chapter looks at the relationship between privacy and freedom of expression in the context of the media. Privacy is an important right; it is an aspect of human dignity. But freedom of expression and particularly expression by the media are cornerstones of pluralistic democracy. These two powerful human rights are often in conflict, the resolution of which can mean the limiting of one right in favour of the other.

We begin by looking at the ways in which privacy is currently protected from media intrusions by legislation and regulation, from the Human Rights Act 1998 to the Data Protection Act 1998, and the industry's regulators, Ofcom and the Press Complaints Commission. We then examine how case law has evolved in this area to further protect invasions of privacy by the media.

The second section in this chapter examines the shortfalls present in the current landscape of privacy protection, analysing how effective legislation and regulation have been in addressing the right to privacy, and how well they strike a balance between this and freedom of expression. We then evaluate the development of case law, with particular emphasis on whether the recalibration of the traditional breach of confidence action is apt in this area.

In the third and final section of this chapter we explore the ways in which the current position might be reformed to better strike the balance. Should Parliament legislate for privacy in the media field, or is it better for the courts to develop the law in this area? We also look at potential reform of the regulatory system and the availability of legal aid and/or conditional fee agreements for privacy claims.

Before embarking on any exploration of privacy and the media, the concept of privacy itself requires examination. The idea of what is private, and as such worthy of protection, is difficult to capture. The right to privacy might be translated as the right to be let alone, or the right not to suffer unwarranted intrusion by the world at large. This right is essentially predicated upon the value of personal identity, and the desirability that this should in some respects be insulated from the outside world. A right to privacy protects fundamental aspects of the self: autonomy, individuality, integrity. This right is an essential component of our humanity. The private zone is the point from which we manage our own

lives and control our engagement with individuals and society. It gives us space to expand and contract such engagement according to the context, and our capacity to negotiate its terms.

Personal identity by its nature is something that belongs, reflexively, to the individual. The right to privacy has a proprietary texture, intrinsically connected to the level of control we exercise over the dissemination of information about ourselves. Effective exercise of the right allows us to decide what information we choose to divulge to whom, and in what form. It is from this basis that we form relationships with other individuals and discover and develop our individuality. This empowerment often marks out privacy as a vital component of personal liberty and dignity, concepts entrenched in traditional notions of democracy.

Freedom of expression, like privacy, is often seen as essential to democracy. Indeed, some see it as the most important human right: guarantee freedom of expression, and all other human rights will thrive. Freedom of expression applies to the dissemination of information and ideas, including those which may be offensive or even harmful. It also extends to the right to receive information and ideas. It is of vital importance in sustaining a free and impartial press, the medium by which society learns about matters of public and political interest, as well as those of a commercial or artistic flavour. The media may be said to be a bulwark of democracy. But, of course, free expression can invade privacy.

# Overview of the current position

## The Protection of Privacy – Legislation[152]

### The European Convention on Human Rights

The European Convention on Human Rights (the Convention) was drafted after the Second World War and the UK became a signatory in 1953. The Convention provides protection for an individual's private life. Article 8 provides:

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

Two important features of Article 8 are to be noted. First, it imposes not only a negative but also a positive obligation on the state to respect, and therefore to promote, the interests of private and family life. It is this feature of Article 8 that requires the courts to ensure effective protection of privacy in cases where the complaint is of intrusion by a private individual or company. Secondly, Article 8 guarantees "respect for" the interests of private and family life; these words have the effect that only intrusions of sufficient seriousness are within the scope of Article 8.

---

[152] The importance of legislation is underlined by the fact that, as was stated by Lord Walker of Gestingthorpe in *Douglas and others v Hello! Limited and others* [2007] UKHL 21, "[t]his House has quite recently reaffirmed that English law knows no common law tort of invasion of privacy: *Wainwright v Home Office* [2004] 2 AC 406. But the law of confidentiality has been, and is being developed in such a way as to protect private information".

The Article 8 right is qualified, not absolute. Often, one of the limits on Article 8 arises out of the conflicting right to freedom of expression enshrined in Article 10 of the Convention, which is that:

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. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

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, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

Article 10 is qualified by reference to the rights of others, and by the need to protect information received in confidence. Article 8 and Article 10 cross-refer to each other in the way in which each is qualified. This engenders a tension that will be explored in further detail below. The European Court of Human Rights (ECtHR), based in Strasbourg, interprets and applies the Convention.

## The Human Rights Act 1998

The Human Rights Act 1998 came into force on 2nd October 2000 and incorporates the Convention into English law. The rights incorporated (some Convention rights are not) include those enshrined in Articles 8 and 10 and are set out in Schedule I of the HRA. Prior to the implementation of the HRA, English law recognised no free-standing right of privacy, although on occasions causes of action such as trespass or breach of confidence were used to protect certain aspects of privacy. Under section 2 of the HRA, when determining an issue that has arisen in connection with a Convention right, the English courts are required to take into account any relevant Strasbourg jurisprudence, including judgments, decisions, declarations or advisory opinions of the ECtHR; but the HRA does not give direct effect to Convention rights. This has meant that, in order for the right to privacy to be recognised in disputes between individuals, English courts have had to interpret the provisions of the HRA in a manner that allows it to be recognised as a right at common law.

The HRA protects individuals against unlawful interference of their Convention rights by the State and it is, therefore, not possible for a private individual to institute proceedings against another solely on the basis of breach of a Convention right. An individual must have a legitimate cause of action under English law. The HRA provides that it is unlawful for a public authority to act incompatibly with a Convention right. The HRA does not define what a public authority is. However, it does provide that the English courts are public authorities for its purposes. The HRA further imposes a requirement on English courts to interpret, as far as is possible, legislation compatibly with Convention rights. Where primary legislation is deemed incompatible with a Convention right by a court, that court may make a declaration of incompatibility.

The HRA gives individuals who claim that a public authority has acted incompatibly with a Convention right the option to bring proceedings under the HRA in the appropriate court or tribunal, or to rely expressly on the Convention right in question in any legal proceedings. These provisions, along with related case law, fashion an indirect protection of Convention rights as between

individuals, often referred to as the horizontal effect of the Convention. This has, as will be seen below, had a significant effect on the law of privacy in the UK. Whilst a claimant cannot bring an action against another individual for a violation of Article 8 rights alone, it is possible to use existing rights of action as a vehicle by which to advance the protection of privacy in the UK. This has enabled individuals to gain redress in respect of invasions of privacy, though it has conversely resulted in the unfortunate distortion of certain existing causes of action.

In addition to the incorporation of Article 8 of the Convention, other provisions of the HRA are relevant to the protection of privacy and freedom of expression. Section 12 of the HRA applies when a court is considering whether to grant relief that may interfere with freedom of expression. Section 12 compels the court to consider the merits of an application before granting an injunction to restrain publication of certain material. It must be satisfied that an applicant is likely to establish at trial that publication should be restrained. In this regard, the court is further required to respect the importance of freedom of expression, whilst at the same time affording the same regard to any relevant privacy code. That Parliament intended freedom of expression to occupy a special position within the matrix of freedoms in English law is clear. Equally manifest is Parliament's apprehension of the tension between freedom of expression and both libel (which we are not discussing here) and the right to privacy. The crux lies in how the freedom and the right can be satisfactorily reconciled in each case. It is left for the courts to weigh the balance. Parliament has adopted this pragmatic solution. From the point of view of the media, English courts tend to be harsh task masters. This can introduce a tension with the pro free speech element in Strasbourg jurisprudence and can exacerbate the collision with the right to privacy, another human right in an arena where neither has inherent primacy.

## The Data Protection Act 1998

The Data Protection Act 1998 (DPA) implements the 1995 EU Data Protection Directive and regulates the storage and usage of information about individuals. The provisions of the DPA should be considered wherever the media publishes, or intends to publish, information about an individual. The *Naomi Campbell* case, discussed below, shows that the DPA can be the media's undoing in a privacy case.

In effect, the DPA applies to all personal data processed by a data controller on a computer or held in a highly-organised manual filing system. Where the data controller is a public authority a much wider range of "unstructured" filing systems is covered. The DPA expressly recognises sensitive personal data, which includes personal information about racial and ethnic origins, political beliefs, religious or other beliefs, membership to trade unions, physical or mental health, sexual life, the (alleged) commission of any offence and any proceedings for any offences committed, their disposal or sentence.

The DPA sets out eight guiding principles by which all personal data must be handled. To compress the wording of the DPA, personal data must be:

(a) fairly and lawfully processed, and in particular;

(b) processed for limited purposes, which purposes usually need to be notified to the individual concerned;

(c) adequate, relevant and not excessive;

(d) accurate;

(e) kept for no longer than is necessary;

(f) processed in line with individuals' rights;

(g) secure; and

(h) not transferred to countries outside the EEA and several other approved countries without adequate protection.

With regard to preventing or limiting invasions of privacy by the media, these provisions will be relevant where the media use surreptitious means by which to obtain information about an individual, for example by using a zoom lens, or by committing or using the fruits of, for example, theft, trespass, breach of confidence or any unlawful act in order to gain the material. The principles may apply where the media reveals information about an individual where the disclosure is disproportionate to the reasons for releasing the information. This may be particularly relevant where photographs are used. The media must also be careful to ensure that any material stored or revealed about an individual is accurate to avoid falling foul of the DPA.

Under the DPA, all personal data must be fairly and lawfully processed. "Processing" personal data under the DPA means obtaining, recording, holding, transferring, or carrying out any operation on the data. Whether personal data has been lawfully processed is perhaps more readily ascertainable than whether it has been fairly processed. Schedule 2 of the DPA assists in this regard, setting out conditions which are relevant in the processing of any personal data. At least one of these conditions must be satisfied for data to be deemed processed fairly. With regard to sensitive personal data, at least one of the conditions in Schedule 2 *and* at least one of the more restrictive conditions set out in Schedule 3 of the DPA must be met.

Section 10 of the DPA entitles an individual to give written notice to a data controller to cease, or not to begin, processing personal data under certain circumstances. These are that the processing of the data or the manner or purpose for which it is processed is likely to cause unwarranted substantial damage or distress to the individual or another. Section 13 entitles an individual who suffers damage, or, in the case of processing by the media, distress, to claim compensation.

Section 32 of the DPA provides an exemption from the data protection principles (save for the seventh, concerning security) if:

(a) the data is processed with a view to publication by any person of any journalistic, literary or artistic material;

(b) the data controller (this means a person who determines the purposes for and the manner in which personal data are, or will be, processed) reasonably believes that, having regard to the special importance of the public interest in freedom of expression, publication would be in the public interest; and

(c) the data controller reasonably believes that compliance with the data subject's rights and the principles is incompatible with the special purposes of journalism, artistic and literary purposes.

This exemption applies before and after publication, and is therefore capable of being used as a defence in respect of material that has already been published. Article 2 of the Data Protection

(Processing of Sensitive Personal Data) Order 2000 allows the processing of sensitive personal data for journalistic, artistic or literary purposes relating to a wide range of conduct, for example, unlawful acts, dishonesty and incompetence. The processing must be in the substantial public interest.

### The Protection of Harassment Act 1997

The Protection of Harassment Act 1997 (PHA) establishes criminal and, in some cases, civil liability for a course of conduct that amounts to harassment of another or two or more people. The PHA provides an exemption under section 1(3)(c) if it can be shown that the conduct alleged to be harassment is reasonable in the circumstances.

Although not precisely defined in the PHA, the definition of harassment allows a liberal application by the courts. As such it extends to "harassment" by the media, and could include several forms of investigative journalism, such as "doorstepping", which may also amount to trespass, and also the publishing and broadcasting of material. In this regard, any instance where a broadcast/publication occurs more than once, the journalist/media organisation may be subject to the criminal and civil sanctions imposed under the PHA. Furthermore, the PHA provides no guidance as to whether harassment for the purposes of reporting material would be deemed to fall within the exemption relating to 'reasonable' conduct as set out in section 1(3)(c). As such, the PHA provides a platform, albeit through the ambiguity of certain defined terms, from which judicial interpretation may determine the extent to which individuals should be protected from such conduct. The PHA also has the potential to address the fundamental harm at the heart of an invasion of privacy in that it focuses on the nature of the intrusion itself, and not simply the information or knowledge obtained from it.

In a case[153] brought by an individual against *The Sun* newspaper, the publication of articles by the newspaper, which were foreseeably likely to cause the claimant distress and stimulate a racist reaction on the part of readers, was a course of conduct amounting to harassment under the PHA. Further, in order to determine whether in any individual case harassment was established, the publisher is now required to consider whether a proposed series of articles likely to cause distress would constitute an abuse of freedom by the press. The pressing social needs of a democracy require that such abuse should be curbed by the State.

### The Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIPA) sets out the terms upon which the interception of public and private communications will be an offence. RIPA regulates both postal and electronic communications and includes emails. RIPA may have relevant application in the context of surreptitious recording of, for example, the telephone conversations of public figures.

## The Protection of Privacy – Regulation

The regulatory codes are important for two reasons. First, they have an effect in themselves in the areas they regulate. Additionally, the courts are obliged under the HRA, as outlined in paragraph 15 above, to pay particular regard to any privacy code when considering whether to grant any relief that may limit freedom of expression.

---

[153] *Thomas v News Group Newspapers and Another* [2002] EMLR 4 CA.

## Ofcom Broadcasting Code

The Ofcom Broadcasting Code (OBC) regulates broadcast media and replaces the Independent Television Commission and the Broadcasting Standards Code. Section 8 of the OBC sets out provisions in respect of privacy. The purpose of the section is to ensure that broadcasters avoid "any unwarranted infringement of privacy in programmes, and in connection with obtaining material included in programmes". This wide-ranging principle means that the OBC addresses the methods by which material is captured, as well as the nature of the broadcast itself.

Broadcasters are required to justify that an invasion of privacy is warranted. If a broadcaster claims that the invasion is warranted because it is in the public interest, it must be able to demonstrate that this prevails over any right to privacy. Examples of the public interest under the OBC include revealing or detecting crime, protecting public health or safety, exposing misleading claims made by individuals or organisations or disclosing incompetence that affects the public. Notably, the OBC does not define exhaustively what is deemed "warranted", so an invasion of privacy may be justified in circumstances other than those in the public interest.

The OBC makes particular reference to two forms of intrusive mechanisms used in order to collate materials for broadcast – "doorstepping", which is defined as the practice of the filming or recording of an interview or attempted interview for broadcast, without any prior warning, and "surreptitious filming or recording".

In order to make a complaint alleging an infringement of privacy to Ofcom, certain criteria must first be met.

(a) The complainant must have a direct interest in the subject matter of the complaint;

(b) The matters complained of must not be the subject of legal proceedings in the UK, or be more appropriately resolved by legal proceedings in the UK; and

(c) The complaint must not be frivolous.

Should a complainant be seeking an interim injunction in respect of material that is to be imminently broadcast, this would preclude a complaint under the OBC.

The OBC recognises that private acts may take place in public places, in effect, that a reasonable expectation of privacy may arise even in a public place. This expectation, which is consistent with ECtHR jurisprudence, is checked by limiting principles such as: (i) the nature of the information, act or condition in question; (ii) whether the complainant is a figure in the public eye (although, as we shall see, the ECtHR draws a distinction between public figures who have a political or public role or office, and those such as celebrities who do not); and (iii) whether the information is in the public domain.

If the OBC is breached, Ofcom will publish an adjudication and explain the basis for its finding. If a broadcaster deliberately, seriously or repeatedly breaches the OBC, Ofcom may impose statutory sanctions against the broadcaster including fines and even in some cases revoke the broadcaster's licence.

## The Press Complaints Commission

The Press Complaints Commission (PCC) regulates print media and was set up in order to provide a route of redress in respect of complaints against the press. It is funded by the press and made up of members of the press and a majority of lay members appointed by an independent Appointment

Commission. The PCC Code (the Code) addresses unwarranted infringements of privacy by the press. The Code is reviewed periodically by the Code Committee. All of the members of the Committee are drawn from the press. A breach of the Code that cannot satisfactorily be resolved between the parties through mediation may lead to the offending party being required to publish the PCC's decision in its newspaper or magazine with due prominence.

Many of the provisions of the Code refer to privacy. Paragraph 3 of the Code mirrors the wording of Article 8(1) of the Convention. Paragraph 3(ii) of the Code expressly states that it is "unacceptable" to photograph a person in a private place without obtaining consent from that person. A note to paragraph 3 provides that public property may be deemed a private place where there is a reasonable expectation of privacy.

Paragraph 4 of the Code prohibits harassment, intimidation or persistent pursuit and provides that editors must ensure this principle is followed by their employees or others working for them and to be careful not to use "non-compliant material from other sources". Paragraph 5 deals with intrusions into grief and shock, and paragraphs 6 and 7 address the protection of the privacy of children. Paragraph 10 provides that the press must not publish or seek to obtain material that has been acquired by using clandestine methods. It additionally states that obtaining information through misrepresentation and subterfuge can generally only be justified in the public interest and only if the material cannot be gathered by any other means.

Paragraphs 3, 4, 6, 7 and 10 – among others – in the Code are subject to a public interest defence that may be utilised by the press. The relevant provision states that a public interest defence may subsist in the following non-exhaustive situations, namely:

(a) detecting or exposing crime or serious impropriety;

(b) protecting public health and safety; and

(c) preventing the public from being misled by an action or statement of an individual or organisation.

The press must show that the public interest has been in some way served by its actions; it is not for the complainant to prove that it was not. The PCC will, like Ofcom, consider to what extent the material is in already in the public domain. Notably, and not surprisingly for the press' code, the Code also recognises that there is a public interest in freedom of expression as a free-standing concept, a privilege that is not accorded to an individual's right of privacy. This notion of how private rights have traditionally been restricted by public interest arguments is explored further below.

## The National Union of Journalists Code of Conduct

The National Union of Journalists' Code of Conduct (NUJ Code) sets out the main principles of British and Irish journalism, to which journalists joining the NUJ must subscribe. Many of the provisions of the NUJ Code mirror those of the PCC Code. The NUJ Code contains similar provisions in respect of privacy, accuracy, clandestine methods of gathering information, children and intrusion into grief and shock. There is no provision relating to harassment. Under the NUJ Code, clandestine methods of gathering information, intrusions into private life and into grief or shock may be justified in the public interest, although the public interest itself is not defined. This Code is important because the ECtHR has repeatedly emphasised that Article 10 only protects journalists who comply with the ethics of journalism. The Code is likely to be regarded as a source of guidance on such ethics.

## Other Ways to Protect Privacy

It may be possible to utilise other causes of action to protect privacy in certain situations. A complainant might be able to bring claims in public or private nuisance (the former perhaps only in very limited circumstances) or for trespass to land and/or to the person. Malicious falsehood and defamation might also be relevant in redressing invasions of privacy, however, neither will be appropriate if information that is revealed about the complainant is not false.

Where information that is revealed through an invasion of privacy is false, but not defamatory or injurious, how could a claimant seek redress? If it was not possible to institute "false privacy" claims in this situation, a complainant would have less protection if the information revealed was false, than if it were true.

## A Stand-alone Tort of Breach of Privacy?

The protection of privacy in the UK has come about largely through the development of case law, rather than by legislative or regulatory means. It is helpful to consider how this protection has evolved by analysis of the relevant case law in this area.

In *Kaye v Robertson and Another*[154] the Court of Appeal confirmed that in English law there was at this time (prior to the HRA) no right to privacy, and hence no right of action for breach of privacy. In this case a famous actor sought to prevent *The Sunday Sport* from publishing an "interview" and photographs taken while he was recovering from a road accident in intensive care, after a journalist and photographer gained access to his hospital room. He had not been fit to consent, and had not consented, to the interview. Having no specific right to privacy, Kaye could rely only on claims for malicious falsehood and passing off. Ruefully, the Court of Appeal perceived their ill-fitting nature and commented that it was now desirable for Parliament to consider how to protect an individual's right to privacy.

Ten years later in *Secretary of State for Home Department v Wainwright*[155], the Court of Appeal and House of Lords confirmed the absence of a specific tort of invasion of privacy and reiterated that it was for Parliament, and not the courts, to delineate the "proper ambit" of protection in this area. The case concerned a mother and her son who were subjected to a humiliating strip search when they went to visit a member of their family in prison. They both experienced emotional distress and the son suffered from post traumatic stress disorder. The incident took place before the HRA had come into force. This meant that the Wainwrights could not rely on the provisions of the HRA that would have allowed them to bring proceedings in the domestic courts against the Home Office in respect of the breach of their Convention right to privacy. The matter progressed to the House of Lords where it was reiterated that there existed no general cause of action in English law for an invasion of privacy, capable of providing the Wainwrights with a remedy under English law. The Wainwrights eventually succeeded in Strasbourg, where the ECtHR held in September 2006[156] that there had been a violation of Article 8 (privacy) and Article 13 (effective remedy).

---

[154] [1991] FSR 62.

[155] [2002] QB 1334 (CA) and [2004] 2 AC 406 (HL).

[156] Application No. 12350/04.

## Breach of Confidence: the Protection of Privacy through the Back Door

While the courts have generally been unwilling to recognise a new tort of invasion of privacy, they have been prepared to carve out some protection by utilising the traditional breach of confidence action. It is helpful to consider the three elements of this action, as established in *Coco v AN Clark (Engineers) Ltd*[157].

(a) The information subject to the alleged breach of confidence must have the necessary quality of confidence;

(b) The information must have been imparted in circumstances importing an obligation of confidence; and

(c) There must be an unauthorised disclosure or use of the information.

There must be some existing information upon which to mount an action for breach of confidence. Often this information can be extremely valuable. One of the more memorable cases to be heard soon after the coming into force of the HRA was the application for an interim injunction in *Douglas and others v Hello! Ltd*[158]. The claimants, a well-known celebrity couple, made an agreement with *OK!* magazine to publish carefully selected pictures of their forthcoming wedding and reception. At the event photography, other than by the official *OK!* magazine photographer, was strictly prohibited. The claimants subsequently discovered that, in spite of this precaution, surreptitiously obtained photos of the wedding and reception were to appear in *Hello!*. The claimants applied for and were granted an interim injunction on the basis that publishing the photos would be a breach of confidence. The defendants appealed, and it is here that we can see how the Court of Appeal drew on the traditional action for breach of confidence to address privacy concerns.

Although the injunction was lifted, the Court of Appeal judges, with differing degrees of emphasis, suggested that English law would now recognise and protect where appropriate a right of privacy. However, the majority were concerned to locate the available protection in the equitable doctrine of breach of confidence. It was already settled law that, in relation to the second of the requirements for breach of confidence, it was no longer necessary for there to be an express confidential relationship between confider and confidant. A duty of confidence will arise where a person is in receipt of information that he fairly and reasonably knows or ought to know is confidential[159].

The Court of Appeal advanced further here. It stated that, even where there is no relationship or deemed relationship, the law should nonetheless protect those who have suffered an unwarranted intrusion into their private lives, and not only those who have suffered an abuse of trust. The concept of privacy was for the first time distinguished as a legal concept capable of affording protection in respect of an individual's inherent autonomy. However, the reliance on the law of confidence was confusing and unhelpful.

That the confidential or deemed confidential relationship could now be dispensed with formed the basis of the justification for the imposition of an indefinite injunction against the defendant and the

---

[157] [1969] RPC 41.

[158] [2001] QB 967.

[159] *Attorney General v Guardian Newspapers Ltd. (No.2)* [1990] 1 AC 109

world in *Venables and another v NewsGroup Newspapers Ltd*[160]. This was in order to prevent the media's disclosure of information which may have effectively identified the killers of James Bulger. It could not be argued that there was any special relationship of confidence that would be subverted by the disclosure, and yet the injunction was granted, freedom of expression constrained, and the breach of confidence action expanded as a result.

The stage seemed set for the courts to recognise an action for breach of privacy in its own right. Case law had developed sufficiently and, together with the HRA, which expressly recognises the right to privacy, cut what many would deem a clear path towards this recognition, and yet the courts declined to take this route.

In *A v B plc and another*[161], which concerned an appeal against an interim injunction preventing the defendant from publishing a kiss and tell story about the claimant the court was confident that the breach of confidence action would generally provide adequate protection of an individual's privacy. It was not considered necessary to "tackle the vexed question" of whether a breach of privacy should give rise to a separate cause of action entirely distinct from the law of confidence. Ironically, this dismissal of the issue served merely to highlight the necessity of broaching the difficulty.

Unfortunately for the Douglases, when their claim went to trial in 2003[162], the court was similarly loathe to explore the possibility that there may be a separate cause of action for breach of privacy. But the court awarded damages to the claimants for breach of confidence. Again, the issue of Parliament's reluctance to better define privacy protection was noted by the court. It was recognised that, unless Parliament acted soon, it would be up to the courts to fashion effective privacy protection incrementally, with all the attendant delays, confusion and uncertainty that might result.

## Exploring the Concept of Privacy

Perhaps this climate of uncertainty related in part to the fact that, even at this point in the 21st century, the legal definition of privacy was very much in its nascency. Even now there is no exhaustive or definitive guidance (if this is at all possible) as to what is private and what is not and, by implication, when Article 8 should be engaged. Common sense may assist in this regard. Most people would have little trouble distinguishing facts relating to, for example, medical information, finances and information relating to children as private. Further, activities that take place within a certain sphere, such as the home or a doctor's consulting room, are likely to be deemed as private. The concept is dual-pronged, comprising elements in relation to the functional or thematic – what the activity or information is and/or what it relates to, and the spatial – where the activity takes place or from where the information originates.

Can an activity that takes place in a spatially uncontroversial sphere, such as in public, be private? Two cases heard in the ECtHR went some way towards clarifying the issue:

The applicant in *Peck v UK*[163] was filmed by CCTV walking along a street with a kitchen knife in his hands. He then attempted to commit suicide by slashing his wrists. The footage did not show Mr

[160] [2001] 1 All ER 908.
[161] [2003] QB 195.
[162] [2003] 3 All ER 996.
[163] [2003] E.M.L.R 15.

Peck cutting his wrists, it merely showed him in possession of a knife in the aftermath of his suicide attempt. The local council published press releases including two still photographs and an accompanying article, to illustrate the power of CCTV to prevent potentially dangerous situations. The story and one of the photographs were also published in two local newspapers, and subsequently broadcast by Anglia Television and by the BBC. Mr Peck's identity was not specifically masked in any of the publications or broadcasts. Mr Peck made a complaint to the Broadcasting Standards Commission ("BSC") and the Independent Television Commission ("ITC") alleging an unwarranted infringement of his privacy. The BSC complaint was upheld. Anglia TV accepted that it had breached the requirements of the ITC code and the ITC held that Mr Peck's identity had not been sufficiently obscured. Mr Peck also made a complaint to the PCC, which decided that, because the event had taken place in public, an infringement of privacy could not have occurred. Mr Peck's further application for judicial review of the council's decision was rejected because the council could not be deemed to have acted irrationally in releasing the footage. Further, the court held that there was no general right of privacy under English law. Mr Peck appealed to the ECtHR.

Mr Peck was successful in the ECtHR, which defined private life in broad terms. It was held to encompass such elements as gender identification, name, sexual orientation and sexual life. The right to privacy was also held to protect the right to establish and develop relationships with others and, notably, the right also covered professional or business activities. The ECtHR referred to a "zone of interaction with others, *even in a public context*, which may fall within the scope of 'private life'" (emphasis added)[164]. Note here that the reference to relationships and zone of interaction does not necessarily presume that an individual will form relationships and interact with others. The emphasis here is on the right of an individual to control their mode of engagement, if any, with the world. This control is an essential element of independence and, by implication, privacy. The ECtHR found a violation of Article 8 because of the wide publication of the image in question. Although Mr Peck must be assumed to have expected that a few passers-by would see him, he would not have anticipated the publication of his photograph in the mass media.

This idea of a zone of interaction was taken up in *Von Hannover v Germany*[165]. The applicant to the ECtHR in this case was Princess Caroline of Monaco, who had been the subject of intense paparazzi scrutiny for much of the 1990s, with even the most trivial aspects of her daily life reported in the press. Princess Caroline complained about a series of photographs that appeared in German magazines, depicting her going about her daily life in public. She argued that publishing these pictures infringed her right to private life. The German courts held that she could not assert a right of privacy in a public place and because she was a public figure, there was a public interest in knowing how she behaved in her daily life.

The ECtHR disagreed. It referred to the zone of interaction an individual has with others cited in *Peck v UK* and added that private life includes "a person's physical and psychological integrity"[166]. Interestingly, the ECtHR alluded to privacy as a right that can be eroded through continued intrusion, making what appeared to be a thinly veiled attack on the paparazzi. This led some commentators to suggest that the principles established in *Von Hannover* would only apply in cases of press

[164] Ibid. at paragraph 57.
[165] (2005) 40 EHRR 1.
[166] Ibid. at paragraph 50.

harassment. However, the ECtHR has since applied those principles to cases which have not involved any element of harassment [167], and this wide interpretation of *Von Hannover* has been adopted in domestic law by the Court of Appeal in *McKennit v Ash* [168]. Significantly the ECtHR said that Member States might have, along with a duty to provide remedies in respect of breaches of privacy, positive obligations to prevent breaches of privacy. The concept of the "margin of appreciation" under European law will still be relevant. When the ECtHR determines whether interference with a Convention right is necessary, proportionate and meets a pressing social need, it will allow the domestic courts a measure of discretion in their initial assessment. This is because domestic courts are thought likely to be better placed to make this judgement.

Critics of the decision in *Von Hannover* have pointed out that Princess Caroline was pictured in public and in situations that could hardly be described as private. Hers was not a *Peck* situation. The ECtHR has, therefore, effectively declared a willingness to protect, in certain circumstances, public acts that take place in public. The media might ask where one draws the line between public acts that can be protected and those that cannot. The privacy that is being protected is elusive in definition. The media inevitably see this as an unwarranted restriction on what has long been its territory. If the press is open to censure on such wide grounds it may be that they will be less inclined to fill its role as public watchdog in situations where a clear public interest cannot be shown. *Von Hannover*, which as already noted has been adopted and applied in domestic law, represents a restrictive formulation of where the balance between freedom of expression and privacy should be struck, particularly in its analysis of what is in the public interest, which will be explored in further detail below.

## The Misuse of Private Information

One of the most significant privacy cases to come before the English courts is *Naomi Campbell v Mirror Group Newspapers Ltd.* [169]. This case concerned two articles published by the *Mirror* newspaper about Campbell's drug addiction and treatment. At a previous interview during which the subject of drug addiction was discussed, Campbell had unequivocally denied using drugs. The information contained in the articles was divided into five categories by the court. They were:

(a) the fact that Campbell was addicted to drugs;

(b) the fact that she was receiving therapy for her addiction;

(c) that the treatment was at Narcotics Anonymous;

(d) details of the treatment; and

(e) a photograph showing Campbell leaving a Narcotics Anonymous meeting.

Campbell accepted that she could not claim redress in respect of the publication of the first two categories of information, as she had previously lied to the public about taking drugs and the press were, therefore, entitled to correct the misleading image that she had presented to the public. In respect of the last three categories of information, Campbell claimed that the publication infringed

[167] See e.g. Sciacca v. Italy (2006) 43 EHRR 20.

[168] [2006] ECWA Civ 1714.

[169] [2004] 2 AC 457.

her right to privacy and was therefore a breach of confidence. She also claimed that the publication was in breach of the DPA.

At first instance Campbell was successful on both heads of claim. It was held that details regarding Campbell's attendance at Narcotics Anonymous possessed the necessary quality of confidence, and Campbell was entitled to keep them private. The court considered that even self-publicists should be entitled to keep some information private. Further, the information disclosed was held to be sensitive personal data under the DPA. The *Mirror* could not avail itself of the exemption under section 32 of the DPA because it did not apply post-publication.

The *Mirror* appealed and the Court of Appeal reversed the decision, considering that the information contained in categories (iii) – (v) was merely peripheral to the first two categories. It held that, where publication of confidential information was justifiable in the public interest, reasonable latitude as to the way in which information was presented should be given to the publisher. If this method of presentation were restricted, this would constitute an unnecessary inhibition on freedom of expression. The Court of Appeal also held that the publication came within the exemption set out in section 32 of the DPA, even though it appeared from the wording of the Act that the exemption would apply only before material is published, hence the wording "with a view to publication". The Court reached this construction of section 32 after referring to Hansard, and because it could see that the narrow interpretation adopted by the trial judge would mean that there would be no defence to a DPA claim in most cases where the complaint was made about the publication of personal information.

Campbell was given leave to appeal to the House of Lords and won the appeal by the narrowest majority: their Lordships were split three to two. The divide illustrates the inherent difficulty faced by the courts in determining claims relating to the invasion of privacy. Indeed, it conveys the fundamental complexity of the question of how far a right can be restricted for the purpose of according due protection to a conflicting right. Nonetheless, their Lordships went some way towards tackling the vexed question of how privacy should be protected under English law, grappling with the murky position under existing precedents, Strasbourg jurisprudence and the delicate mechanics of Article 8 and Article 10. A framework intended to govern privacy claims was advanced.

The court must determine whether Article 8 has in fact been engaged. The first question to be determined is this: does the complainant have a reasonable expectation of privacy in respect of the material disclosed? If the answer is no, then the court need go no further. If the answer is yes, the court must secondly conduct a balancing exercise between Articles 8 and 10. In weighing up their relative importance, the court must recognise that neither right has pre-eminence over the other. What has been seen as the presumptive primacy of freedom of expression has now been removed from this evaluation. Analysis of the comparative importance of each right within a fact-specific framework should take place. Interference with either right must be necessary and proportionate – the court must consider the benefit of protecting one right against the potential detriment caused by limiting the other. In effect, the consequences or significance of interference with either right must be weighed against each other.

This is a delicate test – freedom of expression and privacy are not blunt, black and white concepts: some material is without doubt private, just as some news should without doubt be reported. However, this is not always the case. There are different types of freedom of expression, as well as grades of privacy. That the reporter should have a degree of latitude in decisions regarding what,

and in what form, material should be published still holds true. This is a vital component of freedom of expression. It is essential that the courts should not have total, homogenising control over the style and substance of a journalistic work. The idea of control over information and the way in which it is presented is, therefore, entrenched in both freedom of expression and privacy.

The majority considered that Campbell's right to privacy in this case outweighed the *Mirror*'s right to freedom of expression, deciding that receiving treatment for drug addiction should attract the same level of protection as treatment for any medical condition. Further, divulging details of the treatment had the potential to adversely affect Campbell's recovery process. The *Mirror*'s publication of the details of Campbell's treatment and particularly the accompanying use of a photograph was held to be in breach of confidence as the publication of the material infringed her right to privacy. However, little was said about the DPA element of the claim; the parties had accepted that this claim would follow the outcome of the main claim.

Quite radically, where it relates to an invasion of privacy, the breach of confidence action was described by Lord Nicholls as follows: "the essence of the tort is better encapsulated now as the misuse of private information". It was also firmly established that individuals involved in disputes with other individuals or private bodies can utilise the provisions of Articles 8 and 10, just as those individuals involved in disputes with a public body. This is because the court, as a public body, has a duty to act compatibly with Convention rights.

Some mention should be made of photographs. There was a division of opinion in *Campbell* as to whether a photograph can constitute a more serious invasion of privacy than a verbal description. The majority of the House of Lords considered that a photograph is capable of such impact: as the saying goes, a picture can tell a thousand words. The PCC here, however, does not accept that photographs are innately more intrusive than written material. It considers that it is the nature of the information, and not the way in which it is conveyed, that should be the focus of the determination of whether a breach of privacy has occurred[170].

In 2005, *Hello!* Magazine appealed against the decision of the High Court in *Douglas*, as referred to in Page 82 above. The Court of Appeal had little difficulty in concluding that the unauthorised wedding photographs portrayed private aspects of the Douglas' life and fell within the law of confidentiality, as expanded to cover private information in *Campbell*. The court determined that the action for breach of confidence was not a tort but an equitable action. This may seem at odds with the position taken in *Campbell*.

Photographs were again singled out for special protection. The court considered that the available defence of showing that information was in the public domain may not apply to photographs because each fresh publication and/or additional viewer may cause fresh distress.

The Court of Appeal held that the law of confidence would cover the Douglases commercial interest in the private information contained in the photographs. The law of confidence would protect the opportunity to profit from personal confidential information in the same way as it protects the opportunity to profit from, for example, trade secrets. But the court clarified that the rights in private or confidential information are not transmissible as property rights. The concept of developing image

[170] Press Complaints Commission Annual Review 2005.

rights (a right recognised in France, for example) may be something that the courts need to address in the future, as celebrities continue to trade on their images.

Unfortunately for *OK!*, the Court of Appeal decided that any duty of confidentiality attached only to the authorised pictures of the wedding. Accordingly, *OK!* could not claim for breach of confidentiality in respect of the unauthorised pictures of the wedding.

*OK!* appealed to the House of Lords[171]. Having garnered modest damages for what could now be deemed a virtually unanswerable case for invasion of privacy, the Douglases took no part in the appeal. *OK!* had neither a claim for invasion of privacy, nor could it rely on any parasitic right arising out of the Douglases rights. Traditional breach of confidence was the subject of the appeal.

*OK!* won the appeal. In a heavily divided judgment, the House held that an obligation of confidence attached to any photographs of the wedding, not just to the authorised photographs. The Douglases were in a position to impose such an obligation of confidence: information about the wedding in photographic format was information of a commercial value over which the Douglases had sufficient control. *OK!* had paid £1 million for the benefit of this obligation of confidence and the House could find no conceptual or policy reason as to why its interest should not be protected.

*Hello!* argued that once the authorised pictures were published, they were in the public domain and no longer confidential. The Lords considered that it was necessary to look at the nature of the material in question (in this case, information about the wedding where every picture was capable of attracting protection). There may still be benefit in providing protection, even where material has become public. This will depend on the facts of each case.

Whilst Campbell and the Douglases were championing their privacy rights in the UK, the Wainwrights were plotting a course that would lead them to the ECtHR. While the case does not concern the media or the disclosure of information about an individual as in *Campbell* or *Douglas*, it is highly significant in respect of what the ECtHR said about the level of privacy protection in the UK.

A breach of the applicants' right to privacy was found by the ECtHR, which also noted that Article 8 protected the right to family life (which included visiting a relative in prison). The protection of privacy extended to the safeguarding of physical and moral integrity. Crucially, the ECtHR found that the absence of a general tort of the invasion of privacy in English law had resulted in a breach of Article 13 of the Convention, which provides that an individual who has suffered a violation of a Convention right shall have an effective remedy in a domestic court. The decision in *Wainwright* may have far reaching implications in relation to the protection of privacy in England. Although Article 13 is not incorporated into the HRA, the English courts are bound by the HRA to take account of Strasbourg jurisprudence when determining questions arising in relation to Convention rights. *Wainwright* is the clearest signal yet that a tort of the invasion of privacy should now be recognised in the UK.

## The Public Interest Justification

The public interest defence or justification is one commonly employed by the media to justify invasions of privacy. There is no exhaustive guidance as to what may be in the public interest and courts need to approach the question on a case-by-case basis. It is settled that it is in the public

[171] [2007] UKHL 21.

interest for the media to prevent the public from being misled by the remarks or actions of public figures (see *Campbell*, above). It is also in the public interest for the media to expose crime or protect public health or safety. Is it, however, in the public interest for the public to know about an individual's private life solely on the basis that they are a public figure or otherwise famous? The position under privacy case law was somewhat confused until recently when the ECtHR in *Von Hannover* held that a fundamental distinction needed to be drawn between material capable of contributing to a debate of general interest to society, relating to, for example, politicians and the exercise of their functions, and details of the life of an individual who does not exercise any official functions. The court effectively made the distinction between what is in the public interest and what is merely interesting to the public.

A disclosure will be in the public interest if it contributes to a debate of general interest. This might be argued to be rather a restrictive definition of the public interest. It would certainly put paid to the proliferation of popular kiss and tell stories and articles relating intimate details about celebrities' private lives. The obvious difficulty with the public interest justification lies in the interpretation of debate of general interest. Construing it too narrowly runs the real risk of restricting investigative journalism if the media, keen to avoid censure, stick to "safe" subjects. This in turn will threaten the press' role as public watchdog and may potentially mean that subjects of significance to the public will go unreported.

In *McKennitt v Ash*[172] the claimant, a Canadian folk singer, brought an action against her former friend and business partner to prevent her from publishing a tell-all book about her private life, containing information about her business affairs, relationships and emotional well-being. The defendant claimed that the book was in the public interest because it showed that the claimant did not, in her own life, abide by the "rules" she had published on her official website. At trial, the court held that, in order for the public interest justification to be brought successfully to bear in situations such as this, a high degree of misbehaviour on the part of the claimant should be shown. On appeal, the position taken by the ECtHR in *Von Hannover* was adopted; it was confirmed that it was necessary to draw a distinction between the vital role of the press as public watchdog and its publishing of news about figures who cannot legitimately be described as public figures in the proper sense.

In *HRH Prince of Wales v Associated Newspapers Limited*[173] Prince Charles claimed for breach of confidence when hand-written journals were supplied to the defendant by a disloyal employee in breach of a contractual duty of confidence. The journals were published by the defendant, which was held to be a clear breach of confidence. The Court of Appeal agreed that the journals were clearly confidential and private. The court added a further dimension to the public interest justification, stating that the test to apply when considering whether to curb the defendant's freedom of expression is not simply to ascertain whether disclosure of the information is in the public interest, but also whether it would be in the public interest for the duty of confidence to be breached[174].

---

[172] [2005] EWHC 3003 and [2006] EWCA Civ 1714.

[173] [2006] EWHC 522 and [2006] EWCA Civ 1776.

[174] Contrast this decision with that of *Beckham v Gibson* (Unreported, April 29) (Ch D). An injunction to prevent the Beckhams' nanny from revealing private details about the couple's life was refused on the ground that the story would be in the public interest. This seems contrary to the reasoning in both *Von Hannover* and *Campbell*. It may be that the thinking was that the couple have benefited extensively from their image as a happily married couple. It appears that even express duties of confidentiality might not be effective in some circumstances.

When the public interest justification is accepted, it presents a powerful defence to an invasion of privacy, even in respect of the most sensitive material. When Michael Stone, convicted of the murders of Lin and Meg Russell, sought to restrain the publication of a report regarding his care, treatment and supervision, the High Court ruled that, although it would constitute an invasion of his privacy, the report should be made available to the public[175]. This was because there was a clear public interest for the public to know about his care and treatment under health professionals, which would not be served by limited disclosure. Further it was noted that the publicity surrounding Stone was a result of his criminal acts and that much of the information was already in the public domain.

## Other Defences

Other defences to invasions of privacy by the media include consent and waiver. Ideally, consent should be written and relate expressly and substantially to the intrusion complained of and/or to the information disclosed. Oral consent will have to be proved by the defendant on the balance of probabilities. An argument of implicit consent, particularly in respect of the publication of sensitive personal data, is unlikely to be effective[176].

Waiver shares some overlap with implied consent. Broadly, it will arise where a person has effectively forfeited their right to privacy in respect of matters that they themselves have publicised. It is not a simple test to employ and does not mean that, where an individual has chosen to publicise certain aspects of their private life, free rein will be given to the media to publish all material that it can uncover in relation to those aspects. This overly simplistic "zonal" approach was specifically rejected by the Court of Appeal in *McKennitt*. The extent to which the individual has commoditized their private life for their own benefit will be relevant to the reasonableness of their expectation of any retained element of privacy, but it is to be borne in mind that selective disclosure of one's private information is an exercise of one's Article 8 rights, and does not impliedly authorise further disclosures by others. This is perhaps significant in relation to celebrities who rely on the media to sustain their careers, without which they would be little-known to the general public.

## Remedies

Remedies for invasions of privacy include an injunctive relief and damages. Clearly the former will be the preference of the complainant. Under section 12 of the HRA a pre-publication injunction will not be granted unless the applicant can show that they are "likely" to succeed in preventing the publication at trial. It has been held that a court must be satisfied that, in all the circumstances, the complainant's chances of success should be sufficiently favourable to justify an injunction[177]. There was considerable doubt and speculation over how this section would be applied. It seems to be viewed as a provision favouring free speech. In the Court of Appeal hearing, which followed the trial of *Douglas v Hello*, it was suggested that the courts should be more willing to grant injunctions in privacy cases because damages will often be an inadequate remedy.

Damages awarded in privacy claims so far have been low, tipping the scales at around a few thousand pounds, although settlements of £50,000 plus have been achieved. The position is

---

[175] *Stone v South East Coast Strategic Health Authority* [2006] EWHC 1668.

[176] See chapter 9, "The Law of Privacy and the Media" edited by M. Tugendhat QC and I. Christie, Oxford University Press 2002.

[177] *Cream Holdings Limited v Bannerjee* [2005] 1 AC 253.

markedly different in defamation cases, where often large sums can be awarded. It could be argued that damage to one's reputation has the potential to persist for the longer term than the distress caused by an invasion of privacy. However, it is doubtful whether this can be measured with any accuracy. It seems likely that damages in respect of privacy breaches will rise in the future[178]. If the right is worth protecting, it may have to be afforded real monetary value.

# Shortfalls in the current position

## Introduction

This section explores the shortfalls inherent in the area of privacy protection, from legislation and privacy codes, to gaps in judicial interpretation and protection of privacy and freedom of expression. We focus specifically on whether adapting the traditional breach of confidence action to address privacy concerns is an effective method of protecting privacy, and the difficulties raised by attempting to define privacy as a legal concept.

## Legislation and Privacy Codes

Legislation in respect of privacy is piecemeal and has evolved reactively, rather than proactively. The HRA is an exception. However, it merely provides a vehicle by which privacy rights may be safeguarded and was perhaps intended to address violations of Convention rights by the State or emanations of the same. Despite this, it cannot be denied that it has played a central role in making possible a new climate for privacy protection. The PHA and the DPA provide very useful platforms from which to launch actions for invasions of privacy. Each is, however, customised with exemptions that might easily be utilised by the media. For example, the exemption (not specifically relating to media conduct) contained in the PHA would potentially allow the media to escape its provisions if reasonable conduct could be shown. The vague nature of this exemption has the potential to allow for a wealth of argument in defence to an allegation of harassment under the PHA.

The exemptions from the data protection principles under the DPA may also assist the media. Section 32 relates specifically to the media and provides for a public interest defence that is doubly strengthened by reference to the general public interest and to the public interest entrenched in the concept of freedom of expression itself. However, the section will not apply where there is no conceivable public interest in the story in question. The section has been held to apply both before and after publication[179]. This seems somewhat odd, as the provisions expressly relate to the processing of data "with a view to the publication by any person of any journalistic, literary or artistic material"[180].

It might be argued that the relevant legislation cements freedom of expression as the point from which privacy is viewed. Does the concept of privacy in English law come ready-packaged with concessions to free speech, rather than these concessions acting as secondary limiting factors on the right? This is a difficult question. One may counter that the need to protect the privacy of individuals is clearly the propulsion behind the enactment of the provisions of the HRA, DPA and PHA.

---

[178] See "Privacy Protection Today – from Abstract Principle to Effective Remedy" by Antony White QC, 5th February 2007.

[179] *Campbell v Mirror Group Newspapers Ltd.* [2003] QB 633.

[180] Information Commissioner Richard Thomas has called for criminal sanctions to be imposed on those that breach the DPA, recommending a maximum two year prison sentence for those who unlawfully obtain or sell the personal information of others. The PCC think that this would be disproportionate.

## Regulation

A free press is vital in a democracy. Executive or judicial regulation can be seen as a degree of state censorship. The alternative is self regulation. Ofcom has a role regulating broadcast media. Print media is self-regulated by the PCC.

The PCC has suffered criticism from commentators and complainants alike. Its make up and funding, coupled with its lack of restraining or remedial powers, foster a belief by some that it is an impotent watchdog over the press. Although the PCC will act as a mediator between opponents to a dispute, it does not conduct hearings in person, making only paper adjudications. This, and a reluctance to decide conflicts of facts and evidence, has the potential to limit the utility of the adjudication process. The PCC does not provide for the recoupment of legal fees, and it has no injunctive power to restrain publication or the future re-printing of material, which can often be the only effective weapons against invasions of privacy. Further, the PCC's effectiveness at providing retrospective redress is questionable, as it has no power to award damages to an injured party and/or to fine the offending editor or publisher. The sanctions at its disposal are arguably weakened by its lack of any legal authority to impose its rulings. This may deter an individual alleging an invasion of privacy from seeking redress, as the material complained of may be further publicised without the potential for effective remedy and vindication.

Some decisions of the PCC have also been criticised for their inconsistency. In *Quigley v Zoo Magazine*[181], the PCC held that consent from a parent did not have to be obtained where a photograph was published of a child making an offensive gesture in a football ground. It considered that, although the photograph engaged questions about the child's welfare and therefore necessitated consent, the ground was a public place with a large spectator and media presence and also the parent had impliedly consented to the photography. This notion of public places somehow generating implied consent overlooks the reasoning in both *Von Hannover* and *Peck*, which establishes unambiguously that mere presence in a public place does not give rise to an implied consent to the waiver of privacy in respect of actions performed within it. The press needs to know before publication whether a disclosure will offend against law or code.

The PCC has reached different decisions in complaints involving similar facts. The PCC adjudicated against *The Guardian* for paying money to obtain a prisoner's diary recounting the time he spent with Jeffrey Archer in prison, whilst, on the same day, it was discovered that the PCC were intending to pardon *The News of the World* for allegedly paying a convicted criminal for providing details on the Beckham kidnap plot. These discordant positions have led some to suggest that the PCC favours the tabloids at the expense of the broadsheets.

In 2000, the PCC found against the newsreader, Anna Ford, when she complained that her privacy had been invaded after pictures of her sunbathing with her children on a beach in Majorca appeared in *OK!* magazine and the *Daily Mail*. The photos had been taken with a long lens camera. The beach was secluded and adjacent to Ford's hotel; she had thought that the beach was private. The PCC found that, because the beach was accessible to the public, Ford could have no reasonable expectation of privacy in respect of actions performed within it. This contrasts with the decision reached in 2007 by the PCC in relation to Elle Macpherson against *Hello!* magazine. Macpherson was sunbathing on a private beach with her children. Pictures of her and her children appeared in

[181] PCC Adjudication, 20th July 2006.

*Hello!*, which Macpherson claimed was an intrusion on her privacy. The agency that took the photos claimed that it believed the beach was not private. The PCC found that Macpherson had a reasonable expectation of privacy and found against the magazine. This apparent inconsistency in approach may be unsettling for the press.

The ECtHR has been receptive towards media regulation, and noted in this context a possible distinction from print media in that it has a more pervasive impact[182]. Ofcom is generally regarded as having more "teeth" than the PCC. Ofcom's decisions do have considerable admonitory value: broadcasters generally respect and follow Ofcom decisions. As a public authority under the HRA, it is required to act compatibly with Convention rights[183]. Unlike the PCC it does have the power to fine a party found to have committed a breach of the OBC, and thus may provide more satisfactory redress when compared with the Code. It is notable that it does not have power to award damages to an injured party, which would perhaps require only a nuancing of the position in relation to its ability to fine. Further, Ofcom does not have any power to restrain publication. This is significant as a complaint to Ofcom is precluded if the matters complained of are the subject of legal proceedings in the UK. Immediate or prompt proceedings may be the only means of restraining publication, which is initially the ideal remedy in cases of invasions of privacy. Even if an injunction cannot be obtained, proceedings may be progressed with a view to obtaining damages. The position may effectively force an individual to choose between initiating court proceedings and making an Ofcom complaint[184].

The old Broadcasting Standards Commission Code provided that invasions of privacy can occur "during the obtaining of material for a programme, even if none of it is broadcast". In contrast, the Ofcom Broadcast Code Guidance specifies that a complaint can be made to Ofcom in respect of alleged invasions of privacy only if the programme in respect of which material was gathered is eventually broadcast[185]. This disregards almost entirely the possibility that privacy can be invaded even where the connected broadcast is not shown. It may be necessary then, for a complainant to utilise the PHA or the DPA in respect of invasions of privacy in this situation. This loophole in the OBC Guidance goes some way to illustrating the tendency to band together invasions of privacy with the resulting information or material gleaned from the invasion. This position, as will be seen below, has often resulted in some confusion as to what the right to privacy actually entails, and, by implication, what constitutes an invasion of the right.

## The Problem with Confidence: a Shift in the Centre of Gravity

We have seen above how the equitable action of breach of confidence has been used to protect individuals from invasions of privacy by the press. This appears to be an unsatisfactory legal conceit, in that it confuses the concepts of privacy and confidence, resulting in the unstable protection of each. Privacy and confidence, although sharing some similarities, are fundamentally different concepts. A claim for breach of confidence has its roots in the confidential relationship and the

[182] Per the decision in *Jersild v Denmark* [1994] ECHR 15890/89 at paragraph 31 "it is commonly acknowledged that the audio-visual media have a much more immediate and powerful effect then the print media"; discussed in *Murphy v Ireland* (application no. 44179/98).

[183] The position with regard to whether the PCC is a public authority for the purposes of the HRA is unclear. The PCC has not officially acknowledged that it is.

[184] See chapter 17 of G. Phillipson and Helen Fenwick's, "Media Freedom under the Human Rights Act", OUP 2006.

[185] See http://www.ofcom.org.uk/tv/ifi/guidance/bguidance/

quality of information, and can be defeated if a defendant can show that the information is false, trivial or in the public domain[186]. This may not be the case with privacy. Further, the existing cause of action for breach of confidence has been destabilised by the judicial contrivance of rendering obsolete the requirement for there to be a relationship between claimant and defendant.

## Loss of the Relationship

The decisions in cases such as *Venables* constituted a dramatic remodelling of the traditional requirement for a relationship of trust to subsist between a claimant and a defendant in an action for breach of confidence. Subsequent decisions on invasions of privacy were often made without the need to grapple with its substance as a legal concept because the facts could either fit neatly into the breach of confidence action, or be shoehorned into it, in that information was usually imparted in circumstances imposing an obligation of confidence. In *Campbell* it could not be said that all of the information concerned was imparted in such circumstances, and the increasingly inconvenient requirement for a relationship was unpicked to impose an obligation in respect of private information where an individual can reasonably expect their privacy to be respected. This appears to stitch too closely together the first and second limbs of the traditional breach of confidence test: the quality of the information now gives rise to a climate, rather than potentially preceding a relationship, of privacy.

This loss of the requirement for a relationship is concerning for the future of breach of confidence actions. Confidence requires an engagement that gives rise to a relationship of trust and mutuality. The right to privacy subsists without the need for a relationship; it is a concept that functions at a more primary level. It is the basis upon which individuals control their level of engagement with the world. Without the need for a relationship just what, one might ask, is said to have been violated by a breach of confidence? If there is no longer a need for a relationship, the law of confidence might lose its value in its traditional area of protection, for example in the area of trade secrets. In some cases it seemed that the focus had shifted almost entirely to the quality of the information itself, with scant recognition of one the tenets on which traditional breach of confidence was based. However, in two recent Court of Appeal decisions referred to above, *McKennitt v Ash* and *Prince of Wales v Associated Newspapers Limited*, the court emphasised that, where a case does involve a traditional relationship of trust and confidence, this will be important both in identifying the information in respect of which the claimant may have a reasonable expectation of privacy and in the balancing exercise where it will point in favour of giving the Article 8 right precedence over the Article 10 right.

## Informational Privacy

That the protection of privacy against media intrusion has developed under the doctrine of confidentiality goes some way to explaining why the protection afforded by the courts often fastens on the disclosure of private material. Often in privacy claims against the media, there is great furore surrounding the information that has been revealed, in minute detail, to the public. This can overlook the fact that, with invasions of privacy, it is often the surreptitious way in which the material has been obtained, along with the feeling of being spied upon, that causes the real distress to the complainant. It is the invasion itself that is the nucleus of the harm.

This becomes all the more apparent in situations where there is an invasion of privacy but, in fact, no information is divulged. Consider the Wainwrights, who each suffered a gross invasion of privacy,

[186] But there may be qualifications to the public domain defence; see page 96, below.

and yet no information was disclosed. After all, there may be no information to disclose. This cannot logically be the position with breach of confidence. Without the disclosure of information, there can be no breach of confidence. Further, an invasion of privacy may not provide new knowledge. If one person knows something about another individual, for example, what birthmarks they may have, it does not mean that watching that person undress to reveal the same is not an invasion of privacy because no new knowledge or information was obtained[187]. Invasions of privacy require an intrusion upon the self, whereas breaches of confidence require the acquisition of information infused with the quality of confidence.

In cases of invasions of privacy where there is no related disclosure of material, a complainant can seek redress through the provisions of the DPA and the PHA. The DPA covers situations where information is processed short of publication, for example, where it is obtained, held or recorded. As outlined above, under the PHA an individual may gain redress in respect of invasions of privacy even where there is no disclosure of information.

## Truth or Falsity

The quality of the information that is the subject of a breach of confidence claim is central to the action. It follows that, particularly in a commercial context, where the information can be shown to be false, there cannot be any claim for breach of confidential information[188]. This is not the case with private information; even if the information divulged is false or inaccurate, it is likely to have been obtained by some form of intrusion, the harm of which may not be ameliorated by its falsity. In *Campbell* it was considered that inaccuracies in the material divulged did not detract from the fact that what had been published was still essentially private. A claimant who is forced to pick through private information in order to tell the court what information is true and what is false, may simply find their distress compounded by the requirement[189]. In *Mckennitt v. Ash* the Court of Appeal rejected an argument that the developing law of privacy could not protect against the publication of untrue private information.

If, however, the information divulged is wholly or substantially false to the extent that there can be no sensible claim to a breach of privacy and/or it is obviously not going to be believed, it is likely that an action for defamation or injurious falsehood should be pursued, rather than an action for invasion of privacy.

The implications for traditional breach of confidence actions are unclear. As the focus here is on the quality of information, it seems logical for a claimant to seek redress only in respect of information that can be shown to be true. Would the traditional action now be expanded to allow a claim to be made in respect of the disclosure of confidential information, some of which is in fact false? This seems problematical.

## Trivia

Trivial information would not be protected under a traditional breach of confidence action[190]. This may not be the case with private information[191]. Relatively anodyne material can still retain its private quality

[187] See N.A. Morgan, "Privacy in the common law: a doctrine and theoretical analysis", 2005.

[188] *Interbrew SA v Financial Times Limited* [2002] EMLR 24.

[189] See for example *Beckham v Gibson* (29th April 2005, unreported).

[190] See *Attorney-General v Guardian Newspapers Limited (No. 2)* [1990] 1 AC 109.

[191] See *Browne v Associated Newspapers Limited* [2007] EWCA Civ 295 at paragraph 33.

if, for example, it originates from a spatially private location, such as the home or a hospital bedroom[192]. It is likely that most people would find the description in minute detail of the layout and decoration of one's home laid bare in a magazine particularly intrusive. The relative immateriality of the weight of the information in this regard once again illustrates that it is the intrusion that is central to invasions of privacy.

On the other hand, the words "respect for" in Article 8 mean that only intrusions which are sufficiently serious in nature will fall within its scope. In effect, the disclosure of private information should be of a level serious enough to warrant redress[193].

## Public Domain

Historically, showing that information was already in the public domain was generally fatal in traditional breach of confidence actions, because it would lack the necessary quality of confidence. In privacy actions a public domain argument may well carry little weight, particularly where photographs are concerned; repeated disclosures of the same information may well cause fresh and even enhanced distress each time[194].

The public domain argument harks back to the reasoning in *Peck* and *Von Hannover* where it was confirmed that private acts might take place in public areas. There is a difference between information being divulged to those physically proximate (this is surely a trade-off we make when *deciding* to engage with society for any reason) and the situation where information may be divulged to a much wider audience without our consent. The difference lies largely in the measure of control the subject is able to exercise on the dissemination of private information[195]. This notion of choice or control lies at the centre of this aspect of the right to respect for privacy, based in part upon independence and self-determination.

It follows that, if the complainant had placed the same or similar information in the public domain then it is likely that they would have difficulty in establishing a reasonable expectation of privacy in respect of it. The extent to which information is in the public domain is also likely to have an appreciable effect on the level of damages awarded in privacy claims.

## The Problem with Privacy – What is Private?

The test for determining what should be deemed private has been outlined above: is it information in respect of which the claimant has a reasonable expectation of privacy? There should be little problem posed by facts which should obviously be viewed as private, and where there is doubt the courts will sometimes look at whether the disclosure would be highly offensive to a reasonable person of ordinary sensibilities in the position of the claimant[196], although this test might not have survived following the decision of the House of Lords in *Campbell*. It is not a threshold test, and should not be used in the first instance to determine whether facts or circumstances are private; it should merely be used where there is doubt. Accordingly, it would not be correct to look at whether

---

[192] See *McKennitt v Ash* ibid. at 174. There was, however, some confusion at first instance about whether triviality would rob information of its private character: some information was held not to cross the privacy threshold because it was too anodyne.

[193] See *M v Secretary of State for Work and Pensions* [2006] 2 AC 91 and *McKennitt v Ash* ibid. at 174.

[194] See *Douglas v Hello! Limited* [2006] QB 125 and *A v B* [2005] EMLR 36.

[195] See chapter 14 of G. Phillipson and Helen Fenwick's, "Media Freedom under the Human Rights Act", OUP 2006.

[196] See *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd.* [2001] HCA 63.

the disclosure of an individual's medical records showing that they had contracted 'flu in the past would be highly offensive to the reasonable person (the chances are that it would not be); the issue here is that medical records are *prima facie* private and the test should not be used. The test is not an easy one to employ. It comprises a mixture of the objective and the subjective. The test is whether the reasonable person of ordinary sensibilities *standing in the shoes of the complainant* would find the disclosure highly offensive. This will be a difficult issue to determine and will depend heavily upon the facts and the relevant history of each case.

The subjectivity element may come into play sooner than at the point of doubt. In establishing whether a complainant has a reasonable expectation of privacy in the first instance, it will be difficult to ignore personal attributes, such as a person being particularly guarded or retiring.

There is no black and white test to determine what is private and what is not. Confidential information does not have the same layered quality that privacy has. Determining what is private is essentially a matter of fact and degree. Taste and decency can often be influencing factors. In *A v B plc*[197] and *Theakston v MGN Limited*[198] the view was taken that information concerning sexual relations within stable relationships is more likely to be protected from disclosure than if the "relationship" were a transient engagement in a brothel. This is despite the fact that the functional aspect of the information, in effect, information pertaining to sexual relations, is the same[199]. This is moral, rather than legal, logic and it is far more difficult to apply to any given situation. Is it the case, then, that the courts are less likely to provide protection from disclosure in respect of information which is questionable on the grounds of taste and decency? Although the courts are not intended to be arbiters of taste, they do appear, on occasion, to judge within the boundaries of what is deemed to be socially acceptable[200].

Perhaps a more appropriate way of identifying where a reasonable expectation of privacy may arise is to look at the functional and spatial aspect of the information or act in question. Where the theme is one that is obviously private, such as sexual relations, grief or medical information, and/or takes place in a sphere to which public access is either prohibited or limited, a reasonable expectation of privacy is likely to arise. This should be protected, unless some countervailing public interest or other defence can be raised.

The decision in *Von Hannover* does not sit well with this formulation. It does seem that the climate of continual harassment featured heavily in the ECtHR's finding of an invasion of privacy, although as noted above this is not the way *Von Hannover* has been interpreted and applied in subsequent ECtHR decisions or in the domestic courts. It remains to be seen whether persistent intrusions upon individuals going about their daily lives in public will be seen to give rise to a reasonable expectation of privacy where the functional and spatial aspect of the information or act concerned is not private.

---

[197] Ibid. at 161.

[298] [2002] EMLR 22.

[199] For a contrasting decision see *CC v AB* [2006] EWHC 3083 (QB), where an injunction was granted to the applicant – a high-profile sports figure – to prevent the respondent from publicising that fact that the applicant had had an affair with the respondent's wife. The respondent made no secret of his desire to exact revenge on the applicant by divulging details of the affair to the public. His motive impacted on the balancing exercise undertaken by the court in the sense that it devalued his Article 10 right in the particular context.

[200] See "Sex, Libels and Video-surveillance", Lord Justice Sedley's Blackstone Lecture to Pembroke College, Oxford, 13th May 2006. See also *Quigley v Zoo Magazine* ibid. at 183.

This would herald a radically prohibitive climate that may even result in the devaluation of the right to privacy, as protection would extend to what cannot arguably be considered private[201].

Harassment in privacy cases was discussed in *Murray v Express Newspapers & another*[202]. The court considered that, whilst it might magnify a "sense and degree of intrusion" felt by a complainant, it was "difficult to see how or why it should be capable of converting an essentially public occasion into a private one".

In this case the writer, JK Rowling, alleged an invasion of privacy had occurred in respect of a photograph of her son with his parents taken as he was pushed in a pram along a public street. Significantly, the facts of this case meant that the court had to effectively choose between what it described as the apparently conflicting reasoning of the House of Lords in *Campbell* – where an act taking place in public was protected because it was inherently of a private nature – and the ECtHR in *Von Hannover*, where it was held that a reasonable expectation of privacy could arise in respect of ordinary, everyday activities taking place in public. The court chose *Campbell*, but with caveats. It was held that, even after *Von Hannover*, there remains an area of innocuous activity which cannot be considered to be private. However, it was accepted that the disclosure of anodyne or trivial information might still be of "considerable importance and sensitivity to a particular person in certain circumstances". This approach means that, essentially, complaints are likely to be considered on a case by case basis. Indeed, whether a reasonable expectation of privacy would arise would be "a matter of fact and degree in every case".

## Article 8, 10 and the Public Interest

The press has historically championed the public interest argument as a defence to invasions of privacy. In traditional breach of confidence cases it has been pointed out that there is a public interest in respecting confidences, and in maintaining confidentiality. There has been limited exploration into the notion that there may be a public interest in the protection of privacy. This may be because, at first glance, privacy may seem the preserve of the individual, relating to autonomy. It allows us to disconnect ourselves from society and, as a consequence, has traditionally been viewed as a concept in diametric opposition to the public interest. Is there a public interest in the protection of privacy? Some commentators (including Liberty) believe so[203], and the arguments expounded serve to inform a more rounded view of both freedom of expression and privacy.

One way in which the protection of privacy can have public value is in the development of relationships. A guarantee of privacy is one of the bases upon which people form bonds with each other; individuals would be reluctant to do so if they knew that every trial and tribulation would be laid bare to the world. This ability to form connections away from, for example, media scrutiny essentially fosters social cohesion and the development of community, both of which are in the public interest.

The protection of privacy may also encourage academic exploration and research, which is in the public interest. A private space may provide a fertile environment within which ideas can flourish (for example, Galileo's?), as opposed to an environment that is scrutinised. There may also be public health issues related to the protection of privacy. For example if someone with a stigmatised infectious

---

[201] See chapter 13 of G. Phillipson and Helen Fenwick's, "Media Freedom under the Human Rights Act", OUP 2006.

[202] [2007] EWHC 1908 (Ch).

[203] See David Mead, "It's a Funny Old Game – Privacy, Football and the Public Interest".

disease, such as tuberculosis, knows that its diagnosis would be made public they may be less likely to seek out such a diagnosis, and would therefore pose a health risk to the rest of the public.

Even arguments advanced in favour of the protection of privacy that appear only to benefit the individual might benefit the public interest. For example, where privacy is undermined or subject to unwarranted challenges, individuals naturally tend to retreat and an environment of mistrust develops. This does not just harm the individual, but society as a whole.

Freedom of expression and privacy are not such distant neighbours from the viewpoint of the public interest. In fact, the concepts may be even more closely linked. Freedom of expression can be dependent on a right of privacy. Without it, true freedom of expression may not exist. It would exist as a freedom that is effectively regulated before it is even exercised, modified for public scrutiny. An obvious example could be found in the development of political ideas and the formation of political organisations, which may be unduly restricted if the individuals involved believed that they could not share ideas within a "safe haven".

There is an accepted public interest argument in preserving confidentiality – by parity of reasoning there is a public interest in preserving the right to privacy. This is, of course, in addition to the fact that privacy – and freedom of expression – are human rights, and the wellbeing of any state requires that all human rights be valued and protected.

# Recommendations

## Introduction

This section looks at the ways in which the protection of privacy rights relating to the media might develop in this context in England and Wales. There are several ways to approach this question:

(a) The HRA is developing privacy – case law already provides adequate protection of privacy rights. No further action needs to be taken.

(b) Legislation is needed in order adequately to protect and clarify privacy rights.

(c) The courts should recognise a new tort of the invasion of privacy, distinct from the traditional breach of confidence action.

(d) Regulation should be strengthened and the task of protecting privacy rights should shift to this arena, rather than be left to the courts or Parliament.

(e) Current methods of funding privacy actions should be reformed.

## The Laissez-faire Approach

Both the courts and Parliament have recognised the individual's right to be let alone and for their personal information to be stored and used appropriately. The law is, albeit incrementally, moving towards increased protection of privacy rights. The incorporation of the Convention on the legislative side, and the recognition that privacy will now be recognised and protected by the courts, have been notable milestones in the area of privacy protection. There is now no presumption that freedom of expression trumps privacy.

But the traditional law of breach of confidence has been stretched by judicial interpretation. Indeed, we have seen what has been described by Lord Hoffmann in *Campbell* as 'a shift in the centre of gravity of the action for breach of confidence when it is used as a remedy for the unjustified

publication of personal information'. The courts have tried to tread a fine line between the two concepts, always alluding to them together and often as inter-dependent. Nevertheless, there appears to be a need for a new apparatus to safeguard each separately – confidentiality and privacy.

## Legislation

The courts have on many occasions called upon Parliament to address privacy concerns at a legislative level. Indeed, cynics might comment that parliamentarians might be the first people to support a law protecting the privacy of the individual. A new Act addressing media privacy would be a bold move for Parliament, but might ultimately prove fruitful. Any legislation would impose rights and obligations between individuals and might further impose an obligation on the State to take positive measures to protect privacy. The question of what facts or circumstances are to be considered private would need to be tackled. It is unlikely that an exhaustive definition could be offered. However, clearer guidance than we now have should be envisaged. Legislation would need to make clear when liability would be triggered – would this be at the point of intrusion or of disclosure of information? If the latter, intrusions and disclosures by the media would come under stiffer censure than other intrusions, such as those where there is no disclosure of information, resulting in a need for a proliferation of legislation. One must question whether it would be in the interests of society as a whole to penalise the media in this way.

Any Act would need to establish the type of liability imposed – this could be civil, criminal or a combination of both. Definition, or at least delineation, of what constitutes the public interest would be needed [204]. In light of Strasbourg jurisprudence on this issue, it is likely that the contribution to the debate of a general interest test would be used. This is retrograde would surely be received with dismay by the press. A list of alternative defences should also be determined.

It is arguable that the above has already been considered and adequately determined by developing case law. The benefit of an Act of Parliament to a complainant, however, lies in the ability to use it as a sword, in order to force a defendant to justify an invasion. The obvious difficulty that remains is the inability of legislation to conduct the balancing exercise between privacy and freedom of expression. Often, it is not a question of whether privacy has been breached, but the issue of how invasion of the right can be justified in context. This requirement is central to the recognition of the competing rights and cannot be conducted other than on a case-by-case basis.

This difficulty was raised by the Government in its responses to the Culture, Media and Sport Select Committee's report entitled *Privacy and Media Intrusion* [205]. The report contains various recommendations as to how the law of privacy might be developed in England and Wales. One of the recommendations made by the Committee is that Parliament should take on its proper legislative role and make legislative proposals in order to clarify the extent and nature of privacy protection. The Committee sees this as necessary in order to satisfy obligations under the Convention.

This recommendation has been met with a negative response. The Government reason that the introduction of privacy legislation is both unnecessary and undesirable, stating that the balancing of free speech and privacy rights is different in every case and therefore the quintessential task of the

[204] The experience of the drafting of the public interest aspect of the Irish equivalent of the *Reynolds*, or *Jameel*, defence in the 2006 an 2007 Defamation Bill suggests that it can be dangerous for a parliament to seek to define such concepts.

[205] Fifth Report of Session 2002-03, Volume 1.

courts. Further the Government considers that any legislation would deem unlawful an invasion of privacy that cannot be justified in the public interest, something which is already a part of the PCC Code. It finds the system of self-regulation an attractive one, observing that court proceedings may further publicise and exacerbate the harm of an invasion of privacy.

## Restatement or Recognition of a new Cause of Action

The courts have inched ever closer to recognising the invasion of privacy as a cause of action in its own right. This has gone as far as recategorising the breach of confidence action – technically an equitable action – as the misuse of private information where it relates to the alleged disclosure of private information. The "new" cause of action exists, although in its inchoate state it might be described as unstable. It has been held by the Court of Appeal that it is not a tort. Recognising the invasion of privacy as a separate cause of action might not be too great a leap of logic for the courts. In fact it might be bizarre at this stage not to recognise it as such. Judicial thinking has manoeuvred itself into a position that demands some form of resolution to the contortion that is now breach of confidence. The action has been rendered neither confidence nor privacy.

Recognition or restatement could be equally effective, perhaps more so, as legislation. A new cause of action has been suggested [206] as one that might consist of the following elements which, if met, would give rise to an action for breach of privacy, namely:

(a) an intrusion

(b) into private life

(c) which would be regarded as highly offensive to a person of reasonable sensibilities.

The intrusion must be unwarranted, or unable to be justified. The "highly offensive" test would ensure that only meritorious claims would be pursued in the courts. One possible difficulty with the above is that the element of objective reasonableness required in (c) will be in some way tainted by the subjectivity arising from the need to place oneself in the shoes of the complainant. But it is clear that privacy is by its nature a notion that is bound to what is personal and subjective.

Conversely, the courts may prefer to maintain their position, albeit now a tenuous one, on the information based relationship between privacy and confidence. Even the courts have recognised the mismatch between the two. Lord Nicholls in *Campbell* stated "the description of the information as 'confidential' is not altogether comfortable. Information about an individual's private life would not, in ordinary usage, be called 'confidential'. The more natural description today is that such information is private'". Considerable effort has been invested in the subsuming of privacy into the breach of confidence action and it would be surprising if the courts recanted completely the complex arguments, structurally difficult though they may be, that hold the two concepts together. It may, therefore, require Parliament to pick up a new broom, and sweep clean. However, for Parliament to sort out the mess would require an enactment to restore the law of confidence, unless the House of Lords finds a way to rescue it.

## Reform of Regulation

Regulators have a unique role to play in the protection of both media freedom and privacy. Unlike recourse to the courts, regulatory resolution has the potential to be less adversarial, cheaper and

[206] See "Privacy and the Media: The Developing Law", Matrix Chambers, 2002.

quicker for all parties. Regulators have shown that they can be understanding of the issues that the media face when deciding whether to publish material, some of which may come well within the sphere of public interest. One of the recommendations made in the Select Committee's report is the introduction of financial penalties for serious breaches of the Code. The Government is reluctant to endorse this view, considering that this has the potential to adversely affect smaller publications. This is a valid concern. However, no consideration was given to requiring offenders to offer an account of profits, or for a sliding scale of fines.

The PCC considers that the admission of the breach of one's own professional standards is enough of a deterrent when it comes to breaching the Code [207]. It also argues that there is no evidence that complainants want compensation for invasions of privacy. In 2006 the PCC published the results of a public opinion survey [208] and found that 68% of respondents would prefer an immediate (thus, the question determined the answer) apology from the offending publication without the imposition of a fine as a remedy for an invasion of privacy. The only other option put forward to respondents was the publication of an apology and the imposition of a fine after a lengthy legal process.

The PCC is reluctant to introduce a remedy for persistent breaches of the Code, stating that the majority of Code breaches are a result of misjudgement or mistake, rather than cynical contravention. This statement might seem curious where offence is caused by long lens photography and surreptitious recordings.

The Government and the PCC are equally loathe to introduce league tables as recommended by the Committee, which would name and shame the worst breachers of the Code. Information on adjudications is available on the PCC's website and the PCC considers that league tables may mislead, in that they would not detail whether the breach was major or minor (though they could), or whether an offer of amends has been made. The Committee's report did not herald any sweeping changes in privacy protection. The more radical changes have been led by the courts.

## Legal Aid and Conditional Fee Agreements

Privacy actions are expensive and often only pursued by those with the deepest pockets. Ironically, these individuals are more likely to have "invited" intrusions by the press than the unintentionally famous. A complaint to the Information Commissioner as the regulator responsible for the DPA may be comparatively cheap, but the cost of court proceedings for an infringement of Article 8 could be prohibitive. As the climate for relatively unknown individuals to be catapulted from obscurity into the spotlight grows, there may arise the need to explore different ways of funding privacy actions without resorting to personal funds.

Legal aid for civil cases has largely been abolished by successive UK governments. It is difficult to see why it should be introduced for privacy claims, unless one argues that Article 6 of the Convention (right to a fair trial) has unique application in respect of breaches of some or all Convention rights, as opposed to its application for any other civil claims.

It is possible to pursue a privacy claim under a conditional fee arrangement (CFA). CFAs allow for the recoupment of a success fee from the losing party to a dispute. CFAs have been heavily criticised by

[207] See Replies to the Committee's Fifth Report, 2002-03 – First Special Report of Session 2003-04.

[208] See Perceptions of the Press Complaints Commission, Omnibus Topline Results, September 2006.

the media. Naomi Campbell fought her claim against the *Mirror* in the House of Lords on a CFA. The *Mirror* challenged the ruling that it should be liable to pay the success fee on the ground that the liability for the uplift was so disproportionate that it infringed its rights of freedom of expression [209].

The Lords found that the payment of the success fee was compatible with the *Mirror*'s Article 10 rights. This was despite the fact that Campbell clearly could have afforded to pursue the litigation using her own funds.

The possibility of having to pay a success fee may have a chilling effect on the media. It may choose to settle a claim even if it has a legitimate defence, rather than incur liability for the success fee. Indeed, it may even choose not to run a story if there is a risk that it may result in litigation and liability for a success fee. The existence of the success fee clearly has the potential to restrict the media's freedom of expression, particularly in the case of smaller publications. Thus, the reality is that it may impact on Article 10 and Article 6 rights.

# Conclusion

Recent decades have heralded a new climate for privacy protection from media intrusion in England and Wales. The courts have formulated the reasonable expectation of privacy test and balanced Articles 8 and 10. With the emergence of the balancing test has come the recognition that freedom of expression does not have presumptive authority over an individual's right to privacy. This shows an appreciation of the importance and utility of both rights. The balancing exercise is key to the resolution of the tension between the two. It also plays a vital role in sustaining the value of each right. Strike the balance too far one way (whichever way that is), and there is not only a risk of damage to the right that is restricted, but also a danger of devaluing the right that prevails.

Analysis of the issues at a micro level can only ever be enriched by clarification at a macro level. At the latter level, it is clear that the invasion of privacy as a cause of action needs now to be distinguished from the action for breach of confidence. Privacy is a constitutional right which protects personal dignity; confidence is an equitable action that protects information and relationships. Whilst the use of confidence to contrive the protection of privacy has provided welcome redress in some cases, it may undermine both rights. It has led to the protection of private information from media disclosure. However, it has left a gap in the protection against intrusions that do not lead to the disclosure of material.

Acknowledgement of the right as one that is distinct from the law of confidence will enable coherent development. Whether it be pre or post publication, the media needs clearer guidance as to when the disclosure of information will be considered to infringe another's right to privacy. It would be a worrying situation for free expression to be restricted simply because the law of privacy is blurred.

The interplay between freedom of expression and privacy shows that these rights are not necessarily in diametric opposition. Whilst the protection of one right may limit the other, both are underpinned by values of control and independence. Both share a public and a private utility. Society needs a clear, fair and effective reconciliation of these rights.

---

[209] [2005] UKHL 61.

# Conclusions

## Introduction

In the introduction to this work we drew a distinction between approaches to differing concepts of privacy. The bulk of the report considers privacy issues traditionally relevant to the relationship between individual and state. Some aspects of mass surveillance, visual surveillance, targeted surveillance and DNA retention cross over into the private sector. However, in the whole, we have concentrated on the public sector. Media privacy is set apart. It is a matter of private law and, unlike other aspects of privacy, has been heavily litigated. As a consequence, since the incorporation of the European Convention on Human Rights (ECHR) via the HRA there has been a development of the common law missing from other aspects of privacy.

Common law interpretation of the Right to Respect for Privacy under Article 8 HRA (along with the intrinsically linked determination of the Right to Free Expression under Article 10 HRA and the common law tort of breach of confidence) has by necessity involved a balancing of competing and potentially conflicting rights. The courts have attempted to steer a path through difficult waters. This is reflected in the conclusions contained in the media privacy chapter which does not make specific recommendations. Rather, the work on media privacy was intended to be self contained. It has identified issues arising from the development of the common law and made suggestions (rather than recommendations) as to how these might be approached. For other aspects of this work however, our findings and recommendations are set out below.

This work was undertaken with the possibility of a single piece of privacy legislation as a potential recommendation. A freestanding Privacy Act might be used to expand and entrench Article 8 while creating an effective enforcement and compensatory framework. The relevance of such a framework would be that infringement into privacy does not often result in quantifiable pecuniary loss. Similarly, as the infringement has already occurred, the relevance of injunctive restriction (the other main disposal open to the court in civil law disputes) is often limited.

However the case for freestanding privacy legislation is questionable. Privacy is such a wide ranging concept that any ‘catch all’ approach is likely to be problematic. It is too much to expect an Act of

Parliament to provide protection benefiting those subject to unwarranted media intrusion as well as those who have suffered excessive targeted intrusive surveillance. It is either likely to be so detailed in providing for appropriate breach, defence and remedy as to be unwieldy, or so broad brush and overarching as to add little to the existing Article 8 framework. A disparate concept such as privacy is essentially context-specific. The appropriate legislative and regulatory response to excessive privacy intrusion is best suited to the specific environment in which that intrusion takes place. For example, the closest thing there is to a 'privacy act' in the UK, the Data Protection Act 1998, provides regulation specific to data privacy.

Therefore, a piecemeal approach to privacy protection would seem the most sensible option. Having said this, it is clear that the range and scope of privacy engagement is increasing to an extent where differing aspects increasing overlap. For example, in the Introduction to Surveillance section, there were a number of references to growing use of data matching and data mining techniques as a response to the increasing data processing automation. Data matching techniques are now being written into legislation such as Part III of the Serious Crime Bill currently before Parliament, while data mining is increasingly being seen as a legitimate tool identifying potential criminality[210]. Although the powers in that Bill are limited to use in criminal fraud investigations, it is likely that the uses of data matching and data mining will expand to cover crime detection generally and possibly into areas other than the detection and prevention of crime.

At the heart of data matching and data mining is the identification of information that is in some way anomalous to other information that is being processed. This raises a series of possibilities once such information has been identified. For example, the process is automated and does not (at least initially) involve human intervention. Once an 'incongruous' data pattern has been established the issue is how to use the information. The investigating authority will be in an interesting position in relation to what legitimate action might follow. It is unlikely that there will be sufficient reason to launch a criminal investigation from a set of unusual data results. Presumably the data received will be one of many sets that might indicate some form of wrongdoing but equally might be absolutely innocent. Regardless of whether the powers to take further investigatory action exist, there might be very good resource and logistical reasons why human input into investigation might initially remain limited.

However, as has been seen in the section on Targeted Surveillance, there were over 439,000 applications for access to Communications Data made under Part I Chapter II of the Regulation of Investigatory Powers Act 2000. As considered earlier, communications data access is available to an extremely wide range of public bodies. It can be self-authorised with the only requirements being that authorisation is in accordance with a range of justifications (including crime detection and prevention) and if the conduct is proportionate to the aim sought. The throwing up of unusual data

[210] As summarised in the Home Office Consultation 'New Powers against Serious and organised Crime' – *'For the purposes of this paper, we see data matching as taking two separate data sets with comparable information (i.e. both contain the same types of information, for example names) and cross referencing them to produce matches. These data sets would typically be for mutually exclusive purposes which can reveal where entitlements are being incorrectly granted, e.g. when the same name appears in connection with pension payments and a list of deceased persons. Data mining, on the other hand, uses more advanced software to analyse data in a number of ways. It can be used within data sets to expose fraud, and is particularly useful when there are many variables within a data set, or the sheer volume of data means that automated analysis is necessary.'* http://www.homeoffice.gov.uk/documents/cons-2006-new-powers-org-crime/cons-new-powers-paper?view=Binary at page 22

patterns arising from data matching or data mining might not justify or legitimise the use of human surveillance or reference to the police for investigation. However, it is more likely to satisfy the more easily achievable requirements of accessing communications data. 'More easily achievable' in this context can be taken to mean both in terms of the legal grounds justifying the accessing of communications data and in terms of the resource that will be necessary to 'investigate' further.

Once an application for access to communications data has been authorised, this will allow access to email, mobile and phone traffic which might take investigation further. If for example, it appears that a series of calls or emails have been made to individuals who are themselves suspected of involvement in criminal activity, then a greater level of intelligence-led investigation might be considered necessary. If, however the communications data does not reveal any unusual traffic, then no further action might be considered necessary. It is, however, extremely unlikely that the person who had had his or her communication traffic studied will be aware of the fact. The sheer number of applications made coupled with involvement after the event limits any practical involvement of, or accountability to, the Interception of Communications Commissioner's office.

Therefore, one potential consequence of growing reliance on data matching practices might be a ripple effect impacting upon the exercise of RIPA powers. The growth of data matching and data mining practices are also likely to raise issues in relation to the way suspicions are recorded. If a pattern of data throws up an anomaly that results in investigation and possible identification of criminal activity, then it is likely that that pattern will be recorded for future reference as flags indicating some sort of impropriety. However, as any two sets of data pattern are unlikely to be identical the indicators are likely to be quite general in nature. As a consequence any similar data pattern is likely to be 'caught in the net' and might warrant further investigation. Again, largely automated processes could have the potential for a ripple effect.

Central to the use of data mining and data matching capability will be the holding of mass informational data. This study has focused on the National Identity Register created by the Identity Cards Act 2006 as being potentially the largest and certainly the most topical example of mass information holding. However, this is only one of many examples. As well as other centralised databases such as the Children Index there are numerous centralised records detailing individual finances, benefit entitlements and so on. Meanwhile the growth of data sale such as with Experian's credit reference database demonstrates increasing reliance on mass data holding in the private sector.

The mass of available data is staggering. As has been said earlier, increasing use of automated sifting is a logical method of identifying potential impropriety. Privacy concerns must be considered in the light of clearly legitimate aims of detecting and preventing crime, protecting children, and so on.

## The legislative framework

Ideally, the legislative environment in which privacy issues arise should ensure proportionality and legitimacy of data sharing and other privacy matters. However, it is arguable that the two main privacy acts, the Data Protection Act (DPA) 1998 and the Human Rights Act 1998 (through Article 8) are unable to keep up with, and by themselves provide sufficient safeguards against, information sharing capabilities.

The HRA is best suited as a means of allowing the individual to seek protection against the excesses of the state [211]. As has been seen, it can be an effective way of ensuring that a celebrity is capable of having their privacy protected from media intrusion. It has also been used successfully when CCTV footage has been inappropriately passed by a local authority to the BBC for broadcast [212]. However, the HRA is limited in use as it necessitates the bringing of an expensive action by a wronged individual. As a consequence, its use in a mass surveillance society is limited. Furthermore, the main tools of recompense for a successful case brought before the European Court of Human Rights or through a domestic court under the HRA are financial damages and preventative action, for example by way of an injunction. Breaches of privacy rarely lead to a quantifiable financial loss. Similarly, injunctive action is often of little benefit as the Article 8 action is likely to have been brought following the alleged privacy intrusion, so the 'damage' will already have been done. Because of the time commitment and potential financial implication of lengthy legal proceedings, the HRA will not always be an attractive or practical option.

The influence of the HRA is not, however, limited to litigation. All new laws are required to be HRA compliant. S.3 HRA requires so far as possible, laws to be read in a way that is compliant with the HRA while S.4 HRA allows courts to make a declaration that primary legislation is incompatible with convention rights. Secondary legislation can be struck down if incompatible with the HRA. This power to strike down secondary legislation is particularly relevant when considering information sharing powers as there is a growing tendency to reserve the detail of sharing for secondary legislation. This was apparent both with the ID Card Act 2006 and the Children Act 2004. The UK Borders Bill, currently before Parliament, creates the framework for a Biometric Identification Document to be issued to non-European Economic Area residents in the UK. This is the first step in the roll out of the ID card regime. Again, nearly every detail on what information can be taken, who can gain access and details of the purposes to which it can be put are reserved for secondary legislation.

In order to confirm that legislation is HRA compatible, every Bill when laid before Parliament must have a ministerial declaration made under S.19 HRA that he or she believes that the legislation complies with the HRA. Given the multiple requirements of Convention article compliance in the HRA, it would be hoped that Article 8 provides significant privacy protection before laws are passed.

This is certainly true to an extent. In particular the Parliamentary Joint Committee on Human Rights (JCHR) , a committee of both Houses set up to consider HRA compliance, will frequently publish reports on legislation as it passes though Parliament. Often its observations on HRA compatibility will be taken on board by the Government and concerns will be addressed before an Act passes into law. However, repeated declarations by courts over anti terrorism legislation incompatibility, for example, show that the Government does not always pay attention to concerns over HRA compliance expressed by Liberty, the JCHR and others [213].

---

[211] Or to require the state to take action to safeguard rights through a 'positive obligation'.

[212] Peck v UK [2003] ECHR 44 (28 January 2003)

[213] Government anti terrorism policy has repeatedly fallen foul of the Courts. In December 2004, the House of Lords Appellate Committee decided by 8-1 that the detention of foreign nationals without trial under Part 4 of the Anti Terrorism Crime and Security Act 2001 breached the HRA. The Control Order Regime set up by the Prevention of Terrorism Act 2005 in order to replace Part 4 has also been declared HRA compatible on several occasions and will inevitably also face final determination by the House of Lords in due course.

The nature of Article 8, as opposed to other Convention rights, also limits its impact both on pre-legislative and post-legislative processes. As argued earlier in considering DNA retention, Article 8's impact will often be widely spread but with repercussions for the individual that are difficult specifically to quantify. This can be contrasted with, for example the Right to Liberty under Article 5 HRA. When Article 5 issues arise, they tend to impact upon a small number of people but in an extremely significant manner. When detention of foreign nationals was introduced in Part 4 of the Anti-Terrorism Crime and Security Act 2001 (ACTSA) or the Control Order regime (which replaced Part 4 ATCSA) was brought in by the Prevention of Terrorism Act 2005 (PTA), they were imposed on relatively few individuals. However, the consequences of detention under Part 4 ATCSA or of being made subject to a control order were extreme. Part 4 detention involved detention in a high security prison. Control orders can result in restrictions up to and including house arrest. The impact upon those subjected to these restrictions was such that Part 4 was made subject to a declaration of incompatibility with Article 5 HRA and other grounds while the High Court and Court of Appeal judgements so far on the PTA have also found the restrictions incompatible with Article 5 and Article 6. If the Control Order regime is finally abandoned, it is likely that the Government, in considering what proportionate and legitimate action is more in accordance with Article 5, will take these multiple breaches into account.

The contrast with Article 8 is pronounced. As noted in the section on DNA, at present no domestic court has acknowledged that the permanent retention of DNA on the NDAD even engages Article 8. While the case of *Marper*, recently declared admissible by the European Court of Human Rights, might determine if Article 8 is engaged, the contrast between the approaches of the domestic courts towards Articles 5 and 8 remains profound.

The Right to Respect for Privacy is just one of the 15 main articles contained in the HRA. The privacy of personal data is a far more significant part of the data protection framework contained in the DPA. The DPA's genesis lies in the European Data Protection Directive of 1995. This, and the DPA itself, set out the framework and principles permitting the retention and dissemination of personal data. The most relevant parts of the DPA are the eight data protection principles and the accompanying Schedules.

As stated in the introduction the essence of the Data Protection principles are:

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be obtained only for one or more specified and lawful purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects.

The Schedules set out the circumstances in which data processing is permitted in relation to data and sensitive personal data [214]. These circumstances include the giving of consent, processing to protect vital interests of the data subject, and processing by public bodies in relation to their work. The DPA also contains exemptions to the data protection principles for purposes such as crime detection and collection, tax collection, national security and health, education or social work.

The DPA has historically proven to be a partially effective mechanism for regulating and controlling the processing of personal data. However, in recent times, further shortcomings are perhaps becoming apparent. The decision in *Durant*, referred to in the section on CCTV, has shown the limitation of scope of DPA in relation to CCTV, although the new draft guidance from the Information Commissioners Office (ICO) does seem to lessen the negative impact. It is also now arguable that technological developments, particularly in relation to the scale of automated data processing possible when data matching and data mining, are outstripping the DPA. To take the second data protection principle as an example: 'data shall only be processed for one or more specified purpose'. The section on Identity Cards mentioned that this principle was being seen as an obstruction to effective information sharing by government departments. Whether or not this is the case, the second principle does not seem well-equipped to deal with mass data processing. At the time of the Data Protection Directive and of the passing of the DPA in the mid and late 1990s, the processing of data was still largely that of single pieces of data for single purposes. There is nothing within the DPA or inherent to the second principle to limit this other than that the purposes for which data are processed need to be specified. This is done by registering the purposes with the ICO. This obligation will not place any significant limitation on data matching practices. Data matching will usually be done for the purposes of crime detection and prevention. If this or any other purpose is notified to ICO, there is no other express limit within the DPA of the scale on which the processing takes place. The Commissioner is given no specific power to refuse an application for notification so long as it is made in the prescribed form. The third data protection principle, that 'personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed' would appear to place some limitation on scale. However, the requirement that data be not excessive would appear to apply to the amount of data relating to a particular individual rather than the number of people who have had their data processed though data matching.

Coupled with concerns over the adequacy of the DPA when applied to modern processing techniques, are the more practical considerations over the ability of the ICO to limit excessive data sharing. There is an inherent limitation upon the effectiveness of a publicly funded body in regulating the public sector. This is no reflection on the work of the ICO, which has frequently drawn attention to privacy issues and highlighted the dangers of the 'surveillance society'. The current Information Commissioner, Richard Thomas, has often demonstrated a willingness to comment on Government

[214] Sensitive personal data is defined by S.2 DPA and relates to data concerning the racial or ethnic origin of the data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, whether he is a member of a trade union, his physical or mental health or condition, his sexual life, the commission or alleged commission by him of any offence or any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

proposals. When giving evidence to the House of Commons' Home Affairs Committee on the subject of Identity Cards, he described their introduction as a 'very significant sea change in the relationship between the state and every individual in the country' [215]. Despite these interventions, the capability of the ICO in regulating the public sector must be limited. Not only is it also a public body but it has resource limitations. The ICO polices not only data protection but also the legal freedom of information framework. The budgetary and resource restrictions under which the ICO operates means its ability to police data protection is necessarily limited.

If the statutory framework and accountability is limited in its ability to temper privacy invasions, then what reform other than a new single piece of legislation would be appropriate? Liberty believes a mix of targeted statutory reform, effective guidance, enhanced enforcement and improved accountability should be at the heart of improved privacy protection within the United Kingdom.

# Findings

Set out below are the main findings of this work. They cover both findings of fact (such as the growth of the national DNA register) and findings of opinion (such as the implications of the growth of the National DNA register). They cover both overarching points relevant to several of the specific areas of study as well as the context-specific findings arising from each section.

## General

1) Possibly the most significant sea change in the nature of information privacy is the blurring of a distinction between historically distinct forms of surveillance. For example, targeted surveillance has typically been interpreted as led by human intelligence against specific individuals or organisations in the course of a criminal investigation. Meanwhile, mass surveillance arguably was not surveillance in a strict sense in that it would not be targeted at any person but involved the retention and dissemination of visual or information data in anticipation of use at a further point. Mass surveillance also covered a wide range of activity covering public service access, state benefit entitlement and so on.

   Demarcation between previously separate forms of surveillance is blurring through the increasing use of data matching and data mining. These activities typically involve automated trawling though seemingly innocuous data to identify anomalous or potentially suspicious patterns. Data matching and mining increasingly are being identified in departmental White Papers as an effective and resource-efficient crime-detection tool. This is filtering through into legislation with the Serious Crime Bill currently before Parliament making specific provision for data matching to combat fraud. Consideration of moves towards data matching and mining should also make reference to profiling. Profiling essentially involves the same data filtering techniques but as yet has not been specifically proposed by the Government as a legitimate and proportionate crime detection device. Profiling is concerned more with identifying information relating to an individual than about details of income, benefits and so on. As a consequence, it is inherently more invasive and touches on more sensitive subject matters such as ethnicity or religion. However, as has been discussed, it is increasingly being referred to as a potentially justifiable method of data filtering, particularly in response to national security concerns.

[215] http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/130/4060801.htm

Use of these techniques makes continued demarcation between targeted and mass surveillance techniques increasingly difficult. Up until now targeted techniques involved the use of RIPA powers (or intrusive surveillance permitted under previous legislation) based on human intelligence. For example, communications data access would be permitted against specified individuals when there were intelligence grounds justifying this. Increasingly, lower-end RIPA powers such as access to communications data might be permitted as a consequence of data matching throwing up an anomaly. This will effectively remove the use of human intelligence involvement until the time when the RIPA authorisation is sought. This is a significant shift.

2) The growth in mass informational data collation and dissemination is increasingly involving transfer across sectors. The two mass informational databases considered in this work, the National Identity Register and the Children Index, both contain provision for access by non public sector agencies. Section 12 IDCA allows for the provision of information from the register to be provided for identification purposes with consent and will provide the means for banks and so on to ascertain the identity of customers. The data sharing regime initially planned for the Children Index in *Every Child Matters* specifically mentioned the 'voluntary sector' as being included of the information hub of agencies allowed access to the register [216]. This inter-sector information transfer is partly a response to societal changes. Traditional distinctions between sectors in recent years have broken down as private-public partnerships have allowed private sector care homes, prisons, health service providers and so on to take on public functions. Meanwhile a growing number of private sector bodies are recognising the commercial potential of data. Collating publicly available information gathered from the electoral register and so on for sale to other private sector bodies can prove highly profitable. Similarly the creation of the Office of the Voluntary Sector has overseen closer links between public and third sector bodies with voluntary organisations increasingly providing services more usually associated with the public sector.

   Increasing contact between differing sectors does not of itself have negative privacy implications. However, it will affect the ability of the ICO to ensure DPA compliance. Separate sectors have differing approaches and attitudes to information. In very general terms, the public sector will view data as being of use for public service provision, benefit entitlement and crime detection. The private sector will tend to look on data as a commodity with either its own inherent value or of use in targeting potential customers. The voluntary sector characteristically views data as a means of identifying supporters or members or of providing benefits or services to its constituent audience.

3) Primary legislation with privacy implications tends to reserve the detail to regulations made later. This trend is not specific to privacy but is characteristic of a general move towards reservation of policy to secondary legislation. However, the implications of this are particularly pronounced in relation to privacy. Details of the bodies given RIPA powers are, for example, contained in orders. Details about the scope of information retention and sharing in the IDCA and by way of the Children Index will be mainly determined though statutory instrument. As has been commented on several times in this work, secondary legislation is a blunt instrument for nuanced proportionality determinations. It is difficult for the legislature to make an accurate determination of whether a particular piece of data can be retained or whether a body should have access to it when regulations cannot be amended.

[216] See footnote 116 above.

4) The legislative framework regulating privacy is unsuited to current requirements. In relation to the DPA this is due to development of the common law (in particular relating to CCTV as a consequence of *Durant*) and as a consequence of increased capability in automated data processing. In human rights terms this is mainly due to the HRA 1998 being ideally suited to provide redress to the individual victim. Inroads into privacy will often have an impact upon society as a whole. However the HRA is not best equipped to provide such a wide analysis. This limitation to HRA litigation is of particular relevance to the rollout of the National DNA database which tends to pit the benefit of solving a specific serious crime against a less quantifiable cost to wider public privacy.

## Intrusive Surveillance

1) RIPA falls short of providing a proper accountability mechanism. The most significant shortcoming is the failure of RIPA to provide any independent judicial scrutiny of applications for intrusive surveillance. Nearly seven years after coming into force, RIPA continues to be criticised for its complexity and the difficulties of interpretation.

2) The regulatory framework for RIPA does not allow comprehensive scrutiny of intrusive surveillance. The Office of Surveillance Commissioners has expressed concerns that the lack of training and awareness among RIPA empowered agencies could lead to unlawful interference with privacy. Reports by the Interception of Communications Commissioner have expressed concern over the numbers of mistakes made during RIPA authorisation. His most recent report also demonstrated the sheer volume of authorisations (over 439,000 in the 15 months between January 2005 and March 2006) making consideration of individual authorisation difficult. This is compounded by the fact that these two surveillance watchdogs mainly operate in a reviewing capacity, commenting on what has happened previously. The Regulation of Investigatory Powers Tribunal also seems unsuited to fulfil a meaningful role in determining complaints. Its inability to consider investigations not authorised by warrant has contributed to a failure to make a single determination of contravention of the HRA or RIPA.

3) The certified warranting process allows the mass examination of external communications (those sent or received outside the UK). RIPA also permits the Secretary of State to authorise certified warranting practices to occur within the UK. It is unclear the extent to which mass surveillance of internal communications takes place.

4) A consequence of increasing reliance on data matching and data mining techniques might result in a knock-on effect increasing the quantity of authorisations of low-level RIPA powers like accessing communications data.

5) The Government has not given any indication that it intends to change the authorisation regime for interception of communications. As a consequence, ministerial oversight is likely to remain in place for the time being. However, there is growing interest in judicial authorisation as evidenced by the recommendation of the Joint Committee on Human Rights in its report on counter terrorism policy that it should be adopted [217].

[217] See Page 36 above.

## CCTV

1) CCTV is more prevalent in the United Kingdom than any other country with an estimated 4.2 million cameras in 2006. New technologies are allowing for techniques such as subject identification, behavioural recognition and subject tracking. Meanwhile CCTV remains poorly regulated, primarily as a consequence of the inherent limitations of the DPA. The logistical ability of the ICO to provide effective oversight of million of systems is also limited.

2) The case for CCTV proving to be a significant crime detection or prevention tool has not been made out. At best it can be shown to have some crime detection benefits when used in conjunction with other crime reduction tools and agencies. Advances in technology do mean that there is potential for CCTV to become a more effective tool of crime detection. Furthermore, it is possible that developments such as subject tracking and sound-enabled systems might potentially result in CCTV having a greater crime prevention impact. However such development also brings the potential for even greater intrusion into personal privacy.

## Mass Data Retention

1) There is a general public acceptance that mass data retention and dissemination might seem an essential aspect of life in 2007. This acceptance is partly due to the necessity of instant availability of information. It is also due to a belief that the holding of information by agents of the state is a necessary prerequisite for the operation of national security. The latter reason is not quite as compelling in 2007 as in the previous five years. While public opinion still appears marginally in favour of mass data retention schemes such as the National Identity Register, support has diminished. This appears to be consequential to ongoing concerns over cost and effectiveness. An inherent trust from a majority of the public in the desirability of mass data retention schemes can no longer be taken for granted.

2) The practicality of mass information schemes still remains untested. Both the National Identity Register and the Children Index remain creatures of statute in that they exist only insofar as determined by their respective Acts of Parliament. The Biometric Identification Document proposed in the UK Borders Bill, which will be used for initial rollout of national compulsory identification has not yet completed passage through Parliament. The NHS centralised health record spine will not require an Act of Parliament as it deals with information already retained on patient health records. However, it is also still some way off coming into operation. While preparatory plans for rollout of these databases are underway[218], there is still some way to go. The next two to three years will be instrumental in determining the full implementation of mass informational databases. As both main opposition parties remain hostile to the NIR the next General Election is likely to determine the NIR's eventual fate.

3) The scope of mass informational databases might need to increase in order to achieve the benefit they have been sold on. This particularly relates to the NIR in combating terrorism or crime. Unless increased levels of information are introduced to the NIR, an individual entry will not contain as much information as will be held by law enforcement agencies. The only way that the NIR could be of greater assistance is if sufficient information is contained to allow a general

[218] Such as by the registration of biometrics with passport application.

level of risk assessment to take place. However, this will effectively amount to profiling of entries. This is a development that would require parliamentary approval (by increasing information contained on the register). It would also raise significant privacy and race relations concerns.

4) The Schedule to the IDCA creates the potential for a detailed audit trail of each person entered on the NIR to be created. The greater the rollout into the private sector the more detailed this will become.

5) The accuracy of entries on the NIR could be improved by improved auditing capability. The IDCA does not contain much detail on self-auditing entries. This is something that might be developed though good practice and guidance.

7) The experience of a compulsory national identity scheme during the Second World War suggests that the range of uses to which the Identity Card will be put is likely to expand over time.

8) The role of the National Identity Scheme Commissioner is limited and does not allow for assessment of the effectiveness and impact of the scheme as a whole.

9) The Children Index has the potential to be a useful tool in identifying children at risk. However, it also has the potential to undermine child protection though excessive entry onto the index resulting in at-risk children being overlooked. It could also have a disproportionate and unjustified impact upon the privacy of children and their families. Again, this might have adverse consequences if it undermines the trust and confidence of relationships between children and health or other service providers.

10) The role and guidance provided by the Information Commissioner's Office will be crucial in determining the effectiveness of the Children Index. In more general terms, the role of the Information Commissioner's Office is of increasing relevance to the operation of mass informational data programmes. Legislation provides the framework but not the operational detail that is crucial in determining both effectiveness and privacy impact.

## DNA

1) A far greater proportion of the United Kingdom's population have their DNA permanently retained on the national DNA database than is the case in any other country. This is due to the grounds for retention being extremely broad and permanent retention being permitted following arrest for a recordable offence whether or not prosecution or conviction follow.

2) A national DNA database is a useful tool for assisting detection of certain types of crime. In particular, it can assist with the detection of offences of violence or involving sexual assault. However, as these only represent a very small proportion of total offending in the United Kingdom, the database has a small impact upon crime detection rates. Extension of the database has not proved to have had a significant impact upon crime detection rates.

3) It has proved difficult to frame debate about the desirability or effectiveness of the National DNA database in privacy and human rights terms. The impact of an advance in DNA resulting in a conviction for a serious historic crime is difficult to compare to the societal change resulting from extension of the database. As a consequence there has been little public debate about the desirability of database implementation.

4) The current sampling scheme is proving discriminatory. There are far more Afro-Caribbean males on the database than any other demographic. A consequence of compulsory retention of DNA for all UK residents would be that it would not discriminate. However, it would represent a significant and disproportionate shift in the relationship between the state and the individual.

# Recommendations

This final section covers recommendations that arise from this report and its findings. It must be emphasised that the policy driver behind public sector privacy intrusion will usually be legitimate. Suggesting that the state generally desires to intrude on privacy for nefarious purposes would be an extreme position to take. There can be little doubt that those in government and other public sector agencies sincerely believe that ID cards will help prevent crime, fight terrorism, deal with unlawful working and migration, with benefit and identity fraud and so on. Similarly, intrusive surveillance, CCTV, and data matching and data mining processes may all be beneficial in combating, investigating or detecting crime. These might be relatively obvious comments to make but are important to bear in mind in determining what appropriate and proportionate steps might be taken in order to safeguard individual privacy whilst still ensuring a public benefit. In the private sector, things are not so clear. A significant motivation mostly absent from the public sector is financial gain. Those who sell newspapers or personal information have no need to justify their activity through identification of some social benefit. As has been noted earlier in the findings, the distinctions between public, private and non-profit sectors are not as clear cut as might have been the case previously. Because of this, the recommendations below are intended to be relevant for privacy regulation in other sectors where appropriate.

## Recommendation: New Data Protection Legislation and a CCTV Act

Liberty has frequently criticised the Government's excessive reliance upon legislation to achieve policy aims. Our concern has been that legislation may be used as a form of 'spin' in order to persuade the public that something is being done to address an issue, even if an Act of Parliament is not necessarily the most appropriate or effective response. Because of this, it would not be appropriate for this report to make recommendations for new laws unless there was a clear and specific need to do so.

There does, however, seem to be a strong case for updated data protection legislation. The first requirement of any legislation should be to establish a solid link between the use of CCTV systems and the application of the existing data protection regime. As considered earlier in the section on CCTV, the case of *Durant v Financial Services Authority* has created uncertainty over the general application of data protection rules, and the governance of the ICO to the use of CCTV. The new ICO draft guidance[219] does seek to redress this by stating that all CCTV systems other than the most basic domestic operation are covered[220]. However, we do not believe that new guidance undermines the compelling case for clarifying legislation. Uncertainly arose over interpretation of the common law. The new ICO guidance is helpful but remains essentially an unenforceable interpretation of the

[219] See footnote 75 above.

[220] The principle in Durant that footage not targeted on a specific individual is not covered by the DPA of course remains.

common law. The benefit of legislation is that it can remove uncertainty. New legislation could also do much to ensure a robust framework and proper accountability. The data protection principles in the DPA provide general guidance over the holding of data but do not cater for specificity over such important issues as the location and marking of cameras, arrangements for access to and destruction of footage, penalties for abuse and so on. What guidance there has been covering these issues has been published by a range of agencies. However, it has been essentially voluntary, unenforceable and dependant on the good will and good intentions of system operators[221].

There have, therefore, been two central concerns over CCTV regulation. First, there has been uncertainty of the application of the DPA to smaller systems arising from the decision in Durant. Secondly, even those systems that are covered by the DPA have only unenforceable guidance providing any detail on the specific application of the DPA to CCTV.

A new DPA could formalise the principle that only the most basic domestic systems are not covered by the DPA. Perhaps more importantly it would allow effective and enforceable regulation. The Guidance provided by the ICO already provides the type of template that could easily be adopted. The purpose of guidance is to ensure that the practice complies with the relevant data protection principles. However, it also effectively fleshes out the appropriate practice in a manner that would be relatively easy to apply in statute either directly onto the face of a Bill or through accompanying regulation.

A good example of this is contained in the ICO's current code of practice when dealing with notification of CCTV system operation. The guidance states:

"Signs should be placed so the public are aware they are entering a zone which is covered by surveillance equipments.
The signs should be clearly visible and legible to members of the public
The size of signs will vary according to circumstances:
For example – a sign on the entrance door to a building society office may only need to be A4 size because it is at eye level of those entering the premises.
For example – signs at the entrances of car parks alerting drivers to the fact that the car park is covered by such equipment will usually need to be large, for example, probably A3 size as they are likely to be viewed from further away, for example by a driver sitting in a car.
The signs should contain the following information:
a) Identity of the person or organisation responsible for the scheme.
b) The purposes of the scheme.
c) Details of whom to contact regarding the scheme.
In exceptional and limited cases, if it is assessed that the use of signs would not be appropriate, the user of the scheme must ensure that they have:
a) Identified specific criminal activity.
b) Identified the need to use surveillance to obtain evidence of that criminal activity.
c) Assessed whether the use of signs would prejudice success in obtaining such evidence.

[221] See for example the guidance issued by the Information Commissioner's Office in 2000 for operators of CCTV systems http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/cctv_code_of_practice.pdf and *"A Watching Brief – A Code of Practice for CCTV"* aimed at public sector users of systems published by the Local Government Information Unit in 1996.

d) Assessed how long the covert monitoring should take place to ensure that it is not carried out for longer than is necessary" [222].

We believe it would be a relatively straightforward exercise to formalise the above into statute.

In March 2007 the Council of Europe's European Commission for Democracy through Law (the Venice Commission) published an opinion on video surveillance in public places and the protection of human rights [223]. This lays out the Venice Commission's views on the data protection and human rights requirements of legislation and good practice governing the use of CCTV. The document is of limited relevance to setting out the detail of any new legislation. It mainly contextualises the data protection obligations of member states as set out by the 1995 European Data Protection Directive 95/46/EC and obligations under the European Convention on Human Rights. In this respect it seems of greater relevance to member states with less developed CCTV cultures, its focus being on countries beginning to adopt CCTV rather than those already with millions of cameras. However it does serve as a useful reminder of the societal impact of CCTV. Cameras have become ubiquitous in the UK and the report provides a reminder restating the ramifications for countries with the human rights and data protection obligations common throughout the European Union. According to the report's conclusion;

*'Video surveillance of public areas by public authorities or law enforcement agencies can constitute an undeniable threat to fundamental rights such as the right to privacy and the right of respect for his or her private life, home and correspondence, his/her right to freedom of movement and his/her right to benefit from specific protection regarding personal data collected by such surveillance.*

*Whilst individuals have a reduced privacy expectation in public places, this does not mean that they waive those fundamental rights.*

*Given the high level of sophistication of CCTV, it is recommended that specific regulations should be enacted at both international and national level in order to cover the specific issue of video surveillance by public authorities of public areas as a limitation of the right to privacy'* [224].

The report's conclusion draws a clear distinction between the existence of data protection laws and the need for further regulation covering CCTV. It emphasises the need for regulation of 'the **specific** issue of video surveillance by public authorities' (emphasis added).

The principal distinction between guidance and legislation is sanction. Guidance is not binding and breach carries no sanction. Obviously legislation (usually) carries compulsion and breach of a requirement can result in civil and sometimes criminal penalties. The creation of any sanction, particularly criminal, should only be introduced in certain circumstances. There should be a clear social need or justification, there should not be any other non-punitive sanction available and the penalty should not be excessive to respond to the need identified. Liberty is not in the habit of suggesting new punitive additions to the statute book. However, there is a convincing case to suggest that the negative societal impact arising from unregulated CCTV use warrants the need for

[222] The current ICO guidance can be found at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/cctv_code_of_practice.pdf

[223] http://www.venice.coe.int/docs/2007/CDL-AD(2007)014-e.asp

[224] Ibid paragraphs 79-81.

legislation to punish failure to conform to requirements. Typically, civil law sanction would be appropriate for breaching statutory requirements. In the example above, from the ICO guidance on location of cameras, breach of requirements on location of notices, notification details and so on could carry a fine. There is an issue over the impact of fines on public bodies. Arguably, they only penalise tax payers. However, fining local authorities is common practice and does carry political consequence by influencing voters.

Criminal penalties are typically introduced for intentional acts breaching confidentiality. The Identity Cards Act, for example, contains criminal sanctions primarily aimed at impropriety on the part of those who handle information on the register [225]. While recourse to the criminal law should always be approached with caution, there might be a similar case made for improper disclosure of or tampering with CCTV material with an intention to cause harm to an individual.

New legislation could also provide for more direct regulation of CCTV by the ICO or create a new office of CCTV Commissioner with functions similar to those exercised by the Identity Cards Commissioner. The case for the creation of a new commissioner function is similar to that for the Identity Cards Commissioner. The role of the ICO is extremely broad, covering both operation of data protection and freedom of information laws. Effective oversight of specific areas of data retention and sharing such as CCTV and data sharing by way of the National Identity Register would require a significant allocation of the ICO's resource if it came within its remit. CCTV operation requires governance on a level similar to that of the Identity Card scheme. A separate commissioner would therefore be justified. In this work we have drawn a distinction between mass informational and mass visual data surveillance. We believe there is also a case for a formal separation of oversight roles. This would allow the ICO to focus attention on the use of informational data, and allow a CCTV commissioner to deal specifically with the substantial regulatory and enforcement issues arising from the millions of CCTV cameras operating in the UK.

The other main purpose of new data protection legislation might be to address problems arising when the existing data protection principles fail to keep pace with increased data matching and data mining abilities. As mentioned previously, when the Data Protection Directive and DPA were passed, technological ability to process mass data was far less advanced than in 2007. As a consequence, the protections offered by the principles are arguably less effective. In order to raise the level of protection to a par with that enjoyed in 1997, a more rigorous analysis of the justifications for data processing would be appropriate.

One approach might be to look at the system of notification of processing by data controllers to the ICO. The present system is governed by Part III DPA and sets out a relatively straightforward system of notification covering the data controller providing basic details such as name and address, nominated representative, the purposes for which data is being processed, a general description of intended recipients, and so on [226]. There is a general prohibition on processing data without registration [227], which is a criminal offence [228], and on changing details without providing notification [229].

---

[225] Section 27 'Unauthorised disclosure of information' and Section 29 'Tampering with the Register'.

[226] Section 16 DPA.

[227] Section 17 DPA.

[228] Section 21 DPA.

[229] Section 20 DPA.

There is also a power for the Secretary of State to appoint data protection supervisors to monitor data controllers' compliance with the Act [230]. These provisions regulate the form of notification but, so long as the process is complied with, have no other impact. The only effective control on processing is contained in Section 22 DPA which deals with 'assemble processing'. This is processing likely to cause damage or distress to data subjects or which might prejudice their rights and freedoms. The definition of what would constitute 'processing likely to cause damage and distress…etc.' is left to parliamentary order. Once a parliamentary order has been made, if the ICO believes assemble processing has occurred he can give notice of his opinion to the data controller and require compliance.

While this might appear to provide some sort of regulatory mechanism, it has not done so. Primarily this is because no parliamentary order has ever been made, so the provisions have effectively failed to come into force. However, even if they had come into force, the way the legislation is structured means that the Commissioner has no power to forbid the processing or require it to be amended until after is has already been carried out. The ICO enforcement powers contained in Part V DPA are restricted to when breaches of the data protection principles have already taken place. By this time the damage may well have already been done.

This rather limited regulatory role fits with the Government's attitude towards notification essentially being a regulatory rather than enforcement tool. As Rosemary Jay and Angus Hamilton point out in Data Protection Law and Practice 'Notification is not a control mechanism; the Commissioner cannot refuse a notification' [231]. The policy driver behind the purpose of notification was set out in the 1998 Home Office Consultation Paper 'Subordinate Legislation: Notification Regulations' which stated *'The Government considers that the primary purpose of notification under the new data protection scheme should be to promote transparency, that is providing to the public and the Commissioner a clear description in general terms of the processing of personal data'* [232] There is no mention of enforcement. As mentioned above data controllers must register with the ICO and processing without registration is a criminal offence. However once registration has occurred there is little the ICO can do by way of enforcement.

It is this notification regime that will govern mass data matching and data mining processes. Application of several of the data protection principles: that data shall be processed lawfully and fairly (the first principle); that it shall be obtained and processed for one of more specified purposes (the second principle); that it shall be adequate, relevant and not excessive for purpose (the third principle); and that it be processed in accordance with the rights of data subjects (the sixth principle) demonstrate the shortcomings of this regime in relation to mass data processing methods. If multiple processing purposes are registered, the second principle will be adhered to. The third data protection principle tends to allow considerable leeway in terms of what constitutes adequate, relevant and non-excessive data in that data matching and mining processes operate on the basis that an extremely broad range of information will be of use in assessing whether or not someone might, for example, be involved in criminality. The sixth principle allows, for example, that processing can be prevented if it would cause substantial damage or distress and if it would be unwarranted

[230] Section 23

[231] Page 246 Rosemary Jay and Angus Hamilton: *Data Protection Law and Practice*. Second Edition. Published by Sweet and Maxwell

[232] Home Office 1998 *Subordinate legislation: Notification Regulations*. No online citation available.

by virtue of S.10 DPA. While S.10 seems to provide further protection under the DPA, it also serves to again demonstrate how data sharing practices have outstripped protections. The Act caters for situations where the processing of a particular piece or pieces of information cause harm to an individual, where they are aware of that harm and are able to request that the processing not take place. This does not match up to the mass processing reality of 2007.

At the heart of a response to these changes in data processing culture should be a significant strengthening of the power and ability of the ICO to regulate the notification process effectively. Notification needs to be more about regulation than about administration. The ICO needs to be able to determine in *advance* whether processing might be constitute 'assemble' processing and take action to prevent it. The ICO needs to be capable of limiting processing purposes, of making decisions on societal rather than individual impact of what might constitute damage or distress, and of strict interpretation of what constitutes excessive processing for purpose. In order to make any of these changes effective, the Information Commissioner needs to be given effective enforcement power to prevent any processing he considers to be incompatible with data protection principles.

Concerns over the effectiveness of the DPA also arise from the definition of 'personal data'. This definition impacts upon the scope of processing regulated by the DPA. The DPA defines 'personal data' as:

*'data which relate to a living individual who can be identified –*

*(a) from those data, or*

*(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller'* [233]

Meanwhile the definition set out in the EU Data Protection Directive states;

*"personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'* [234]

The Articles in the directive are preceded by a series of explanatory 'recitals'. Recital 26 states:

*'Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable'*(emphasis added) [235].

The definition of personal data in the DPA is, therefore, more restrictive than that allowed for in the Directive. The DPA bases the definition of personal data as relating to a living individual identifiable from the data itself or from other information held by the data controller. The Directive is more expansive by allowing the definition to include data identifiable by the controller or any other person.

[233] Section 1(1).

[234] Ibid 87 at Article 2(a).

[235] Ibid 87 Recital 26.

This might seem an obscure and rather academic point. However, it is extremely relevant in the context of the mass data matching and mining processes referred to in this work. We have expressed concerns that pressures towards greater matching and profiling of data might prove irresistible. The definition of data contained in the DPA allows a certain leeway to do this if the data is anonymised prior to passing to a third party for further processing. This would allow, for example, data from the one data controller (data controller 'A') to be passed to another data controller (data controller 'B') to be matched against information held by them. If the data had been anonymised by A before being passed to B (by allocating an identifying number for example) then it might not constitute personal data under the DPA while in B's possession meaning B would not have to comply with DPA requirements. Once B had processed the data they could pass it back to A with, for example, any comment about the person to whom the identifying number related being a potential security or crime risk.

As a consequence the data has not really been 'anonymised' as most people would understand the word. A more accurate definition might 'pseudonymised'. This definition might be used to describe data that does not contain names, but which does contain an identifier (such as a number) unique per individual for some time window. This identifier allows for further information to be obtained which can then be linked back to the person linked to this identifier.

The use of pseudonymised data to allow a way around the DPA would not be possible if the definition in the Data Protection Directive was to be applied. Any processing by B would still have to comply with data protection requirements as the person would be identifiable as a consequence of information held by A.

The implication of this is that it may be possible for data held on the NIR or on other mass informational databases to be matched or profiled against data held elsewhere without reference to data protection principles if it is initially anonymised (even if de-anonymised once passed back). The extent of DPA applicability to anonymised data is a grey area. While certainty in data processing can sometimes be elusive [236], a definition of personal data more in line with the Directive would ensure that 'anonymisation' does not allow avoidance of data protection principles.

Changes such as those outlined above cannot occur without the necessary political will. It is not generally in the nature of a Government to pass laws that restrict its ability to act that increase its accountability or that give powers to other agencies. Certainly, recent administrations have not demonstrated any particular inclination to do so. However political parties can and do act differently if there is a belief that doing so could bring political capital. When the current Labour administration was elected in 1997 it was with manifesto commitments both to delegating power and increasing accountability and transparency. One of the first acts of Gordon Brown as the then Chancellor was to free the Bank of England from political control [237]. Further political decentralisation took place with devolution. The Government also incorporated the European Convention on Human Rights into domestic law though the Human Rights Act 1998. This meant that all public bodies had to act in a way that was compatible with human rights obligations and allowed for the Government's own lawmaking to be considered in terms of Convention compatibility by the courts. The Freedom of

[236] For example, the extent to which those who are passed data by data controllers for further processing are data processors or data controllers can be difficult to define.

[237] http://news.bbc.co.uk/onthisday/hi/dates/stories/may/6/newsid_3806000/3806313.stm

Information Act 2000 was intended to open up the machinations of public bodies to scrutiny by allowing members of the public to request details of their activities [238].

These were the initial acts of an incoming administration sensing political capital to be gained from reversing a perceived lack of openness and accountability in government. Ten years on a similar claim might be made about privacy. Government inroads into individual privacy are a matter of increasing public concern and any party that identifies a need to bolster privacy protection might well gain from taking a bold stance on improved protection.

## Recommendation: Increased Role and Powers for the Information Commissioner's Office

Bolstering the power and resource of the Information Commissioners Office is fundamental to ensuring that there is meaningful regulation of privacy and data protection. The Information Commissioner Richard Thomas has also argued for more substantive powers. In his evidence to the House of Commons' Home Affairs Committee [239] he set out his stall as to what additional safeguards the ICO should enjoy. For the purposes of this work it is appropriate simply to provide a summary of these recommendations. While generally endorsing the suggestions in principle, we do question whether they go far enough. For example, the ICO is updating its code of Practice on CCTV. As we have stated in our main recommendation, we favour substantive legislative regulation of CCTV.

The ICO identifies two work streams; awareness raising and practical measures. Raising awareness might involve new research into public attitudes to surveillance with reference to particular examples such as the creation of the NIR, plans for road user charging and the developments of e-borders.

Practical measures will include the development of an Information Sharing Framework Code of Practice and an updated CCTV Code of Practice. The evidence also identifies scope for improved privacy enhancing technologies which reduce the need to provide identifying particulars in order to access services.

The Information Commissioner also makes a strong case for the use of privacy impact assessments to be provided by both governmental and non-governmental agencies [240]. These would be prepared in conjunction when any new information system is proposed or extension of information sharing planned. As well as offering insight into privacy issues arising from those proposals, they could also allow for privacy assessment to be made by practitioners who are involved in rolling out schemes which have a privacy impact. The Commissioner has also expressed his frustration at the late stage in which his office is involved by central government in its plans and recommends a requirement for his opinion to be sought at an early stage of proposal development.

Arguably the most important suggestions made by the Information Commissioner relate to the powers of his office. He is concerned that his ability to audit and inspect data protection compliance is hindered by the need to obtain data controller consent. He also makes reference to the limitations

[238] It is tempting to add the DPA1998 to this list of decentralising and empowering acts. However, as the DPA was essentially brought in to give effect to a European Directive, this might be a claim too far.

[239] http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/home_affairs_committee_inquiry_into_surveillance_society.pdf

[240] The Surveillance Society report (ibid 4 above) provides further information on PIAs starting at Page 89.

on the effective oversight allowed to his office. Enforcement notices are remedial, fail to punish and are particularly ineffective powers for dealing with negligence or recklessness on the part of the data controller. The Commissioner advocates the need for proactive audit and inspection powers and a more punitive sanction regime.

All the measures suggested would be a positive response to increased use of surveillance. However, they do not address the issue of resources. It is possible that the Information Commissioner did not think it appropriate to address the issue of his office's resource as part of a public evidence session. However, whichever aspect of governmental operation is being referred to, an increase in power will be little more than tokenistic without a corresponding increase in the ability to enforce. This is particularly true in relation to the ICO. There are unlikely to be many publicly funded bodies that have seen their responsibility expanded to a similar extent and who have not also enjoyed a commensurate increase in resource.

## Recommendation: Greater accountability to Parliament

Throughout this work a consistent theme has been Parliament's inability to offer proper scrutiny and oversight of policy impacting on privacy. This is partly an inevitable consequence of the British parliamentary process. A combination of the 'first past the post' electoral system and the structure of Parliament allows for long periods of time when the executive has overwhelming control of the legislature. Between 1997 and 2005 the Labour Party had a massive overall majority in the House of Commons of over 160. This meant that it was extremely unlikely that any of the Bills passing through the House of Commons would face substantial difficulties. Indeed, in the period 1997-2005 the Government did not suffer a single defeat in the Commons. The House of Lords rarely has an overall majority for any single party. However, as the Lords' role is essentially one of review and limited amendment, it is limited in its ability to force substantive change. The Committee system in Parliament will usually have an in-built majority for the party of government so is also limited in its ability to scrutinise. This is not said in criticism of the UK's constitutional system but in order to illustrate how the structure is not weighted in favour of intense scrutiny by the legislature.

In this context there are a number of changes to parliamentary practice and protocol that could allow greater oversight by the legislature. There are perhaps both advantages and disadvantages to a country lacking a written constitution. One of the advantages could be that it is not difficult to change procedures.

At various times in this work reference has been made to problems arising from an inability to amend regulations passed, giving details of, for example, bodies allowed access to communications data or able to access the National Identity Register. This is because, almost without exception, parliamentary orders either require no debate in Parliament (negative resolution) or limited debate where the order will either be passed in totality or fall (affirmative resolution). When the legislation relates to powers of privacy intrusion, the regulation will typically involve a list of bodies to be given powers, access and so on. The problem for parliamentarians is that, while the powers themselves are clearly legitimately exercisable by some bodies [241], they might be excessive for others. A good example of this is the 'snoopers charter', which was an order made under RIPA allowing public

[241] Presumably the powers in the primary legislation would have been voted down by Parliament or declared incompatible with privacy rights through legal challenge otherwise.

bodies access to communications data. When the original list of agencies was published in 2002 it extended access to all local authorities as well as agencies such as the Food Standards Agency and the Royal Pharmaceutical Society.

The problem for parliamentarians is that they might agree to most of the agencies on the list but feel that it is excessive to allow the Food Standards Agency the power to self-authorise communication data access. They would not, however, be able to do anything to prevent this without voting against the entire order. Politically this would be an extremely difficult thing to do given the frequent conflating of privacy issues with national security and crime detection agendas. Few in politics wish to be left vulnerable to allegations of being 'soft' on crime and terrorism.

The rarely used but extremely useful mechanism of the "amendable regulation" could assist. This is written onto the face of the statute and specifically allows for Parliament to amend regulations. It has been used in the Civil Contingency Act 2004 to allow Parliament the ability to determine what constitutes a threat to human welfare in a time of national emergency [242] and in an early version of the Identity Card Bill [243]. At the heart of human rights analysis of privacy considerations is the question of proportionality. Giving parliamentarians the power to amend the regulations would allow a determination as to whether a specific exercise of power is proportionate. If the Information Commissioner's recommendation of privacy impact assessments is taken up, we suggest that any statement accompanying publication of a Bill might include reference to the extent privacy issues can be determined by secondary legislation.

Increased parliamentary accountability could also be achieved by re-designation of the reporting role of individual Commissioners. There are several Commissioners who have specific rolls in assessing the use of privacy impacting powers. The Interception of Communication Commissioner keeps under review the issue of interception warrants issued under RIPA and the adequacy of the arrangements for ensuring the product of interception is properly handled. The Intelligence Services Commissioner is responsible for reviewing the operation of directed surveillance, intrusive surveillance and covert human surveillance powers exercised under RIPA by the security services and other officials such as those of the Ministry of Defence [244]. Rather confusingly a separate body, The Office of Surveillance Commissioners, also has a remit covering the review of directed, intrusive and covert surveillance but this covers general use by policing and other agencies. Finally, when the NIR comes into effect, the National Identity Scheme Commissioner will be responsible for reviewing the operation of certain aspects of the scheme. What this rather bewildering array of oversight bodies share in common is a duty to report primarily to the Prime Minister or to another Government Minister.

It would do much to enhance perceptions of accountability if, (similar to the Information Commissioner [245]), all Commissioners reported directly to Parliament rather than the Executive. This would give both Houses the opportunity to review the Commissioners' analysis of the operational use of the statutory powers they review. At present the reports are published after reporting to the Prime Minister or a Minister, so there should not be any security issues. Such a move might be considered

[242] Section 19 (5) Civil Contingencies Act 2004.

[243] It attached to the order making power compelling specified groups to register. When this Clause was removed from the Bill as part of the compromise to let it pass the resolution power was also removed.

[244] See footnotes 26-28 above.

[245] S.52 DPA.

cosmetic in that it is unlikely that there would be any parliamentary vote. However it would be an important step. It would ensure that parliamentarians had the opportunity for proper debate over the use of powers and would symbolise a shift of accountability away from the Executive.

Accountability to Parliament could be coupled with more rigorous reporting by the various commissioners. The chapter on intrusive surveillance raised concerns over the lack of detail in the current reporting process. For example, the operational use of potentially extremely intrusive mass certified warranting permitted under Section 8 (4) RIPA allowing mass interception of communications, has never been mentioned in the annual reports of the Interception of Communications Commissioner. Parliament may well be more rigorous in its examination of intrusive surveillance practices than the Executive.

Although not a recommendation specifically related to the improvement of privacy protection, it is also worth noting that the oversight structure could be simplified. The basis for having three separate Commissioners seems to be a result of amalgamation of previous oversight regimes to fit in with the structure of RIPA. It is excessively complex and we doubt there are many people, not directly involved with RIPA, who are aware of the structure. We cannot see any reason why separate Commissioners are needed to provide oversight of intercepted communications and targeted communications or why separate Commissioners are needed to oversee directed surveillance from different agencies. A simplified regime would be far preferable.

The use of privacy impact assessments was referred to earlier. They are also worth mentioning in relation to the work of Parliament. At present there are certain impacts of public policy, such as race impact and regulatory impact, which are considered important enough to warrant assessments accompanying Bills when published. The Information Commissioner's assessment of their importance strengthens the case for privacy impact assessments also being made available to parliamentarians and the public.

## Recommendation: Judicial Oversight of Interception of Communications

The section on the operation of RIPA demonstrated a lack of independence in the authorisation process. There is no judicial oversight at all in RIPA. It would be impractical to suggest that there should be independent authorisation when applying for lower level communications data warrants. The hundreds of thousands applied for each year makes this unfeasible. However, high level RIPA powers which rely on Executive authorisation are a cause for concern. In particular it is unclear the extent to which mass certification allowing interception of communications might be operating in respect of internal communications within the UK. These concerns are now being expressed in Parliament by the Joint Committee on Human Rights which has recommended judicial authorisation of intercept warrants.

RIPA requires that the relevant Minister give proper consideration of the need for and the proportionality of each request for an interception warrant. There is no reason to suggest, that any Minister sets out to act in an inappropriate manner. However, the responsibilities of the Executive are diverse and potentially conflicting. There is a wider obligation to the public's safety, to detect and prevent crime and to ensure that state enforcement agencies are able to operate effectively. This range of obligation does not necessarily lend itself to objectivity when determining whether interception is warranted in an individual case.

Even if a Home Secretary were to act in a manner of absolute propriety on every occasion he or she were asked to authorise a warrant, Executive authorisation can lead to allegations of 'rubberstamping'. Without some arm's length independence from the authorising body, there will always be suspicions that proper protocol and safeguards are not being observed. It would be in the interests of both the Executive and the agencies seeking authorisation if an independent judge were needed. It might not always be practical for national security determinations to be transparent. It is, however, possible for them to be seen as more accountable.

While not as desirable as independent judicial authorisation of communication interception, there is a possible halfway house. The Office of Surveillance Commissioners must provide authorisation of any non-urgent use of targeted, directed or human covert surveillance coming within the office's remit. We do not see why a similar need for authorisation should not be applied to intercept warrants requiring non-urgent authorisation by the Interception of Communications Commissioner. Similarly, the Intelligence Services Commissioner could be required to provide authorisation of non-urgent targeted, directed or human covert surveillance in his jurisdiction. The fact that there are a number of Surveillance Commissioners within the Office might provide a logistical, but not a principled, reason why there is currently no authorisation. The appointment of judges in the Offices of the other two Commissioners with authorisation powers would create a similar structure. If the simplification of Commissioner structure suggested above were adopted, a standardised authorisation process could be put in place. Any authorisation by a Commissioner would still not be 'independent' in the full judicial sense. However, it would still be preferable to the current system.

## Recommendation: Extend the role of the Investigatory Powers Tribunal

Prior to Chief Superintendent Ali Dizaei establishing that his phone had been unlawfully tapped, the Investigatory Powers Tribunal had never upheld a complaint. It is difficult to see how any Tribunal where applicants have enjoyed a success rate hovering just above zero can inspire confidence. It is perhaps tempting to explain away this statistic by suggesting that many of those applying suffer from imaginary surveillance by the security services. Certainly the Tribunal is likely to experience a higher number of unfounded applications than most. However, this should not deflect from the fact that large numbers of authorisations of interception take place every year. The Tribunal is hampered by its inability to investigate unauthorised interceptions. It is impossible to say whether these take place or how many there might be. Unauthorised interception is a criminal offence and therefore considered a matter for the police. If a duty were placed upon the Tribunal to refer any suspicion of unauthorised interception to the police, it would provide a mechanism for appropriate investigation.

A Tribunal concerned with surveillance can never operate as openly as other courts. However there are also concerns over the closed nature of the procedure. There is no oral hearing, only limited disclosure of evidence to the applicant and no reasoned decision. The Act specifically excludes access to the High Court to test the legality of decisions. These factors, together with the record of only having upheld one complaint, give rise to a question whether the present system can provide an effective remedy.

## Recommendation: Removal of the Bar on Intercept

Removing the bar on intercepted material in criminal trials is a progressive step that Liberty has been recommending for several years. However, this has usually been in the context of anti-terrorism

laws. We have been concerned that the inability to rely on intercepted material has been used as a justification for the continued operation of quasi-judicial processes such as the use of the Special Immigration Appeal Commission to rule on control orders, and as a justification pre-charge detention of up to 90 days.

Removal of the bar might also have a collateral impact on privacy. It has the potential to impose a degree of self-regulation upon agencies entitled to seek intercept authorisation. The recommendation we have made for independent judicial authorisation of intercept warrants might happen at a future point. However we are unaware of any political will with the current administration to do this. While the current system of Executive authorisation seems set to continue for the immediate future, there is a distinct possibility that intercept evidence might soon become admissible. Senior figures such as the former Attorney General Lord Goldsmith have publicly expressed their support for the move [246]. If this does happen, it raises the prospect that anyone seeking an intercept warrant will have the contents heard in court. There can be little doubt that a warrant will still be sought against anyone suspected of involvement in terrorist activity or serious organised crime. If there is a doubt as to whether authorisation should be sought for less serious investigations, the knowledge that the resulting evidence might be admissible in court might give grounds for hesitation.

## Recommendation: No further extension of powers to retain DNA

Recommendations usually refer to changes to current law, policy and process rather than events that have not yet occurred. However this suggestion is made in anticipation of future developments. In recent years there has been a rollout of the grounds for taking DNA so that DNA can be taken and permanently retained from anyone arrested for a recordable offence. The Home Office consultation *'Modernising Police Powers: Review of the Police and Criminal Evidence Act (PACE) 1984*', which closed at the end of May 2007, indicated that a further extension to cover arrest for non-recordable offences is being contemplated. If this were to occur, it would result in a further massive expansion of the National DNA Database. The greater the percentage of the population on the NDNAD, the closer society is to a point when the case for compulsory national DNA retention can be made. For example in September 2007 the Court of Appeal Judge Lord Justice Sedley argued that the discriminatory impact of the NDNAD justified a move towards compulsory taking and retention of samples from everyone in the UK [247].

Liberty would disagree that there is a compelling case for universal compulsory retention. However, if this is to occur then it is proper that Parliament be given an opportunity to debate the advantages and disadvantages. Such a significant change in the relationship between the individual and the state should also be open to wider public debate. Liberty believes that the current regime is allowing mass rollout of the NDNAD by stealth. There is a danger that extension will eventually lead to a 'tipping point' justifying arguments for a national compulsory DNA database. The UK might be some way from reaching this point. However, the longer roll out continues by stealth at the current rate the greater the prospect of compulsion in the long term.

---

[246] http://news.bbc.co.uk/1/hi/uk_politics/5366430.stm

[247] http://news.bbc.co.uk/1/hi/uk/6979138.stm

## Recommendation: Sample deletion from the NDNAD made simpler

Section 82 of the Criminal Justice and Police Act 2001 amended the Police and Criminal Evidence Act 1984 in allowing retention of DNA regardless of whether a person has been acquitted or even charged. Some police forces do allow for the destruction of samples but this only tends to occur in unusual circumstances. The section on DNA demonstrated that the extension of the NDNAD has not resulted in an increased offence clear-up rate. Similarly there is no evidence to suggest that those who have been arrested but against whom proceedings have not been taken have a greater propensity to commit offences than the population at large. In the absence of any justification for mass retention of the DNA of those who have no criminal conviction or caution, it would be a proportionate step to change the retention regime so that retention continues only in cases where there is a potential crime detention benefit greater than that arising from random selection.

To achieve this, there should be a presumption that anyone who is acquitted of a criminal offence should have their DNA sample destroyed. The same should apply to those who are not charged. This presumption could be capable of rebuttal in certain circumstances. For example, the police should be able to retain the DNA of a person, such as the Soham murderer Ian Huntley, who has come to the attention of police on multiple occasions on suspicion of offences of sex or violence, for the purposes of ongoing or subsequent investigation.

DNA is of use primarily in offending involving sexual assault or violence. It can also be of assistance in detection of some property offending such as burglary. As a consequence, there seems little justification for retaining the DNA of anyone who has not been convicted of these types of offence.

It would be progressive for any administration to take a step to remove the number of samples on the register. It is perhaps too much to expect instant mass deletion of material from the register at this time. Smaller scale staged deletion, for example beginning with the destruction of DNA samples relating to any person under the age of 16 who has not been convicted or cautioned for any offence, should be a perfectly achievable immediate objective. If, however, the potential for use of material on the NDNAD were to expand beyond crime detection purposes – such as use for parental determination – public opinion on continuing expansion may well change.

# Conclusion

This report has followed two broad stands of consideration of the state of privacy in the UK. One has been the relationship between personal privacy and a free media. This has largely been regulated in the courts and has predominantly related not to the public at large but to those in the public eye. The other has been an analysis of the societal privacy impact of surveillance and the increasing use of databases. Recent developments here have occurred not through judicial interpretation but through the introduction of legislation. The lack of judicial determination demonstrates the point made several times throughout this work of the difficulties in enforcing Article 8 rights through the courts.

We have concluded that there are problems arising from the common law development of media privacy and make suggestions as to differing approaches that could be adopted. It is, however, the rise of the ‘surveillance society’ that dominates this work. There has been a fundamental shift in the relationship between state and individual. Without specific action this will continue apace. We have made a series of recommendations that we believe will help restore the balance. We do not seek to

unreasonably entrench individual privacy at the expense of the state's legitimate interests. Rather, we believe that action is needed to reflect the changes that have occurred in the last decade. What we have experienced has largely been one way traffic. Much has affected privacy, but little has protected it. In the introduction to this publication we stated that we believed privacy was a right whose time had come. We hope this report will help persuade others of its importance.

LIBERTY

PROTECTING CIVIL LIBERTIES
PROMOTING HUMAN RIGHTS

The Nuffield Foundation