



ANALYSIS OF THE PROTECTION OF FREEDOMS BILL

-Written By Danny McMahon, Devin Knox and Stephen Hoffman

CONTENTS PAGE

Executive Summary	2
Chapter 1- The DNA Database and Biometric Data Taken From Children	
a) Introduction	3
b) Some Facts and Figures	3
c) Helping the Innocent	3
d) Destruction of DNA Copies	5
e) Discretionary Powers	6
f) Are Police Forces Getting the Message	6
g) Minor Offences	7
h) Those Arrested for Crimes Outside the Jurisdiction of the UK	8
i) Children in Schools: Biometric data	8
j) DNA Retained for National Security	9
k) National DNA Strategy Database Board	9
l) Conclusions	9
Chapter 2- Implications for Surveillance Systems and CCTV	
a) Introduction	10
b) The Story So Far	11
c) Effects on Crime	11
d) State Surveillance Going Wrong	12
e) Government Changes	12
f) The Statutory Code of Conduct	13
g) The Surveillance Camera Commissioner	13
h) Future Implications and Suggested Improvements	14
i) Conclusions	15
Chapter 3 - Implications for the Regulation of Investigatory Powers Act	
a) Introduction	17
b) Interception of Communications	17
c) Surveillance of Private Property	18
d) Monitoring In Public Place	18
e) Covert Intelligence	18
f) Communications Monitoring	19
g) Effects on the Innocent	19
h) Investigatory Powers Tribunal (IPT)	19
i) Intrusion Levels	19
j) Local Councils	19
k) What the Protection of Freedoms Bill Aims To Do	21
l) Suggestions	22
m) Conclusions	22



Executive Summary

- By 2009, nearly 6 Million people in England and Wales were on the National DNA database, many of whom who were either innocent or had only committed minor crimes.
- The database is notoriously inaccurate and bureaucratic.
- The Coalition Government aims to reform the database by generally only retaining the data of individuals who have committed crimes.
- In March 2010, 3,500 schools took biometric data from pupils in order to speed up basic administration. Often the data was taken without parental consent. Crucially, the Protection of Freedoms Bill rules that schools can only take biometric data with parental permission, thus protecting children's rights.
- To improve this further, schools should face punishments if they break the Bill's provisions. The Information Commissioner should also be able to rule if schools are acting in the public interests in relation to biometric databases.
- Whilst the Bill is a step in the right direction, there is much room for improvement. As the Bill stands, adults convicted of recordable offences (even for minor crimes) can have their DNA retained indefinitely. Additionally, the Bill will mean that children can still have their DNA retained indefinitely after two warnings.
- Furthermore, if a person is seen as a national security concern, they are exempt from the protections outlined in the bill. National security exemptions could end up increasing the size of the database unnecessarily.
- Under New Labour, the state's ability to control and monitor its citizens increased exponentially. Most prominent was probably the rise of surveillance systems. For example, despite having only 1% of the world's population, reports suggested Britain had 20% of the worlds CCTV cameras, a staggering 4.2 million.
- The Freedom Bill will allow the Home Secretary to appoint a Surveillance Camera Commissioner.
- They will be a code of practice in respect to the development and use of surveillance camera systems for the police, local authorities and the CCTV industry. This could provide the necessary safeguards, to make CCTV use and surveillance proportionate.
- Unfortunately, any failure to act in accordance to the new surveillance camera code will not necessarily make that person liable to civil or criminal proceedings. This should be enforced more strongly to dissuade people from abusing the code.
- Despite the Bill making some welcome changes, we are worried that due to the pace of technological advancement CCTV cameras will rise just at a slower rate.
- The Bill will make many changes to the Regulation of Investigatory Powers Act 2000 (RIPA) passed under the Labour Government.
- Changes are needed, as under the last Government, RIPA had become a snooper's charter, where many public bodies and local authorities spied on individuals, often for ludicrous reasons.
- The Bill will require relevant authorities to receive judicial approval before accessing communications data.
- The grounds that a judicial approval may be granted include a number of reasons such as economic implications, whether it had done anything to stop crime, and if a person's privacy had been unnecessarily breached.



- This is a great improvement over what RIPA was before, as it will make public bodies and local authorities think twice before abusing surveillance powers.
- This is a step in the right direction, but the criteria for judicial approval are very broad and open to abuse.

Chapter 1: The DNA Database and Biometric Data Taken From Children

- Written By Stephen Hoffman

1a) Introduction

The National DNA Database was created in 1995 by Home Secretary, Michael Howard, from the 1994 Criminal Justice and Public Order Act 1994. It was meant to contain DNA from people who had been convicted of all but the most trivial of offences (Wallace, H, 2005). At present, it entraps many innocent people, which breaches privacy.

1b) Some Facts And Figures

There was an endemic ignorance towards liberty in the previous government's approach to the database. In 2005, the UK had a much higher proportion of its population on a national police database than its international counterparts. For example, whilst over 5% of the UK population was on the database, it was 0.99% in the USA and 0.20% in France (Genewatch UK, 2010). By May 2009, the database had the profiles of 5.5 Million people in England and Wales increasing to almost 6 million when including Northern Ireland and Scotland. This accounts for just over 10% of the UK population (Whitehead, T, 2009).

In July 2010, the National Police Improvement Agency (NPIA) reported a slight reduction in numbers, to approximately 5 Million in England and Wales (NPIA, 2010) which is still a higher proportion than most countries. This meant that under Labour a new profile was added every 45 seconds (Blackwood, N, 2011).

The size of the database makes it immensely bureaucratic leading to security breaches and errors. Rehman Chishti MP has stated that "Half a million records on the database were completely wrong: names and details were false (Chishti, R, 2011)." The database is a threat to liberty and nightmarish to manage.

The database needs to be scaled back to stop freedom eroding. John Glen, a Conservative MP, pointed out that both Conservatives and Liberal Democrats agreed that 13 years of a Labour Government saw a squeeze on civil liberties (Glen, J, 2011).

1c) Helping the Innocent

The retort to those who have concerns about the DNA Database is that much loved phrase "if you have nothing to fear, you have nothing to hide". However, this is simply not the case. According to Jim Shannon MP, as of 24th April 2009, almost 1 Million innocent people were included on the database (Shannon, J, 2011). The National DNA Database Strategy



Board has admitted that presently 20% of those on the Database do not have a conviction (Pugh, G, 2011). As Gareth Johnson MP stated, “Those who preach that if you do no wrong, you have nothing to fear embark on a very dangerous journey where the state is master and the individual is subservient to those in control (Johnson, G, 2011).” The change to allow the retention of the innocent in 2004 paved a way for all police national computer records to be kept permanently (Genewatch UK, 2010). This altered the balance between individual privacy and the ability of the state to implement bio surveillance.

It is extremely difficult to remove DNA profiles. They can only be removed under exceptional circumstances decided by the police. This allows police to enforce and make the law, a clear conflict of interest. Even the exceptional circumstances provision does not save many innocent people as according to Gareth Johnson, “an innocent man is not an exceptional man, his profile could be held on the DNA register for life (Johnson, G, 2011).”

Furthermore, Only 283 innocent people had their DNA samples removed under the exceptional circumstances rule in 2008-9, which is considerably less than Scotland where 16,562 profiles were deleted in 2008-9 (Genewatch UK, 2010).

The situation is serious as according to Genewatch UK, “Individuals with records on the DNA Database lose their presumed legitimacy to go about their daily life, their right to refuse to take part in genetic research and their right to keep their family relationships and other genetic information private. Their movements are also checked, which can have a significant effect on their right to protest (Genewatch UK, 2005).” This is devastating for those who have done nothing wrong. Additionally, there are disparities in the law, because innocent people on the database are treated differently to those who are innocent, but are not on the database.

The European Convention on Human Rights in 2008 for once was correct in the case of S and Marper v United Kingdom (Almandras, S, 2010: 5) ruled unanimously that legislation in England and Wales allowing the indefinite retention of DNA and fingerprints of innocent people breaches Article 8 of the European Convention on Human Rights (the right to privacy).

The Government is proposing provisions so those who are innocent find it much easier to remove their details from the database. Whilst not committed to removing all innocent people from the database, it would like to see a substantial reduction in the number held on it. This will hopefully restore the principle of innocent until proven guilty, which has been badly undermined. The Law Society has rightly described this as an improvement (Brake, T, 2011).

The Government is moving towards the Scottish legal system’s approach where, apart from cases relating to a serious sexual or violent offence, if a conviction does not follow from an investigation or arrest the state cannot retain that person’s DNA (Almandras, S, 2010: 1)



This should make a policeman's job easier, because he will not have to sift through the data of individuals who shouldn't be there.

According to Theresa May MP, present Home Secretary, this will stop innocent people's data being held on the database indefinitely (May, T, 2011).

Mr. Shannon has said that the exceptional cases provisions need to be clarified (Shannon, J, 2011). An amendment could be made to include innocent people under the exceptional circumstances provisions. Thus police would be instructed to recognise the rights of innocent people in law.

Disappointingly, the Government has said it will not remove the DNA of all those who are innocent. Theresa May said, "The police will be able to apply for the DNA of some people who are arrested but not charged to be retained. I would expect that application to be made in certain circumstances, such as when the victim has been vulnerable, which may mean there is very good evidence that the individual concerned has committed a crime (May, T, 2011)." It is commendable to protect the most vulnerable in society, but the loophole could mean substantial numbers of innocent people remain on the database. Thus closing this loophole is recommended.

The Bill should make clear that a right of appeal for individuals who believe their DNA has been retained unlawfully is available. Nicola Blackwood MP, approved such an amendment saying, "I even have one constituent who was inaccurately registered as a sex offender for 15 years owing to a clerical error (Blackwood, N, 2011)."

Furthermore, DNA of those accused of a serious crime but not convicted will see their DNA, with the possibility of it being extended for another two years (Floru, J, 2011). Effectively, they are being treated as guilty until proven innocent. The Government ought to make clear that these people will have their DNA destroyed.

Another problem is once a person's DNA is deleted from the National DNA database, it doesn't specify that it will be immediately deleted from the police's national computer. We believe this should be the case.

1d) Destruction of DNA Copies

The Bill also concentrates on the destruction of DNA copies, demonstrating the Government is willing to relinquish power.

If a valid reason has been given to destroy a DNA sample or fingerprint, then the police have to comply. It is also made apparent that DNA or fingerprints obtained by unlawful means will be destroyed. Hopefully many people will see their profiles removed.

A major problem is mistaken identity. The Government recognises this and has called for DNA mistakenly taken to be removed (Her Majesty's Government (HMG), 2010-11: 9), as it is an affront to justice and expensive.

1e) Discretionary Powers

Presently the database has given police a smorgasbord of discretionary powers. For example, information obtained by the Mail on Sunday, demonstrated that detectives approved by chief constables trawled the DNA database 60 times a year hunting for criminals' relatives. Additionally police have searched the DNA records for innocent people 363 times in the past six years (Lewis, J, 2010). The standard defence is that these searches only happened in exceptional circumstances and that the number is low compared to the number of innocent people on the database. However, the problem is not with who holds these powers, it is that they are allowed to hold them at all. The state was allowing the police to treat people as guilty by association, which goes against equality under the law and challenges the privacy of those subject to surveillance.

The Government has sent a message through a commitment to remove as many innocent people off the database as possible. This will restrict police surveillance operations on innocent citizens.

The Bill is not a panacea to the problem. For instance, chief police officers can carry out speculative searches within such time as is reasonably required (HMG, 2010-11: 2). Whilst the Government intends to stop random stop and search powers, speculative searches of the database could be used. For example, is it really necessary to carry out a speculative search of DNA from those accused of fraud if they are investigating murder. Also a time frame is not specified. These searches should be restricted through tight time limits and exemptions for innocent people. Additionally the search should be restricted to those relevant to the crime the police are investigating. So for example if it relates to a sexual offence, only those who have committed a sexual offence should be searched.

The Bill also says that a Chief Police Officer can ask for a time extension from a magistrate court. This is unnecessary, as 3 years is long enough for a conviction based on a DNA sample or fingerprint. The time could be limited to a year without jeopardising police work. Moreover, a member of the public should be allowed to call for a judicial review when their DNA is held for the time limit to be lowered or profile destroyed. These changes are imperative to stop police acting as if they are above the law.

1f) Are Police Forces Getting the Message

Police forces across the country seem deaf to the new message on DNA profiling. For example, the Derbyshire Constabulary webpage on 17th November 2010, states that "Your authority regularly holds onto DNA samples and fingerprint details even when individuals

have been found not guilty of an offence. Samples etc are only destroyed in exceptional circumstances. (Derbyshire Constabulary, 2010).

This viewpoint suggests police forces are ignorant of potential miscarriages of justice and there is ample room for abuse.

Consequently, new guidelines are essential for the police to act in the public's interest rather than their self-interest.

1g) Minor Offences

In recent years, there has been a proliferation of DNA and fingerprints taken from people who have only been convicted of minor offences, such as being drunk, begging and attending illegal demonstrations.

There are a plethora of case studies outlining the problems. One case involves a fourteen year old girl who had her DNA profile taken for ping-pong a schoolmate's bra (Cunningham, T, 2006). Whilst one does not condone the girl's actions, surely the response was an overreaction. (Cunningham, T, 2006). Angela Hickling, was arrested for theft after a next door neighbour kicked a football over her fence. She could not find it, so could not return it. Later in the day, a policeman questioned her on suspicion of theft. The case was dropped a few days later due to a lack of evidence, but not before her DNA was taken. Similarly, William Copper was arrested and formally cautioned for smoking a cannabis joint in public (Copper, W, 2010). Whilst plainly this is a crime, it is extremely minor. Adding people to the database in these circumstances seems an extraordinary waste of time.

The Government is setting up guidelines to reduce the amount of DNA taken from people for minor offences. This indicates that it is willing to countenance a distinction between minor and serious crimes.

One helpful provision is that people who are arrested, but then not charged or are acquitted of minor offences, will have their DNA records and fingerprints deleted when charges are dropped or an investigation is completed (Genewatch, UK, 2011).

Figures in July 2010, showed over 272,000 individuals under 18 were on the DNA database (NPIA, 2010). Changes to the law will mean that under 18's who are convicted of a single minor crime will have their DNA records and fingerprints deleted after five years, or five years after the end of the sentence if they have been sent to prison. This provides some safeguards (HMG, 2010-11: 6).

Regrettably, the Government plans are not radical enough. For instance, children should be given the most protection under the law. It is wrong that a child convicted of a minor crime should have their DNA held at all. The period of 5 years is still 5 years when the intimate details of a child are held by the state. Furthermore if a child receives committs to minor offences their DNA could be retained for life (HMG, 2010-11: 6). This is



disproportionate, and will cause more children to be involved in the criminal justice system than necessary. Rules ought to be included, stating that children convicted of minor offences must not be added to the DNA database and, if they are, the data has to be deleted as soon as possible.

The Bill still says that the DNA profiles of adults can be retained indefinitely if they have committed a minor crime (HMG, 2010-11: 5). This is massively disproportionate and should be amended to a maximum of two years.

Theresa May has said, “Those convicted of an offence includes those who have been cautioned” (May, T, 2011). Subsequently, these people could have their DNA retained indefinitely, similar to a convicted person. This could lead to the DNA Database being extended, despite the Government wanting the exact opposite. Amendments should be made so those who been cautioned will have their DNA removed from the database.

1h) Those Arrested For Crimes outside the Jurisdiction of the UK

British people can be arrested for something which is not a crime in the UK, but is a crime in a European country like Germany. One such example is holocaust denial.

The Bill says that a person who is convicted of an offence, under the law of any country outside Wales can have their DNA retained indefinitely (HMG, 2010-11: 5).

A Person’s DNA should not be taken if they are convicted of something which is not a crime in the UK. If a DNA sample has been retained, it should be destroyed without delay. This is important, because traditionally the British legal system has far more safeguards, such as habeas corpus, compared to other continental systems. Additionally if the Government does not do this, it is not protecting its own citizens.

1i) Children in Schools: Biometric Data

Children frequently have their privacy infringed upon, when being subject to iris scans to take out library books, often without parental consent. This was all part of a biometric data system, rolled out in 30% of secondary and 5% of primary schools across the UK (Blackwood, N, 2011). Schools have actually accelerated the process of running Biometric Data Systems without consent in response to the Government’s plans to introduce consent into the process according to Terri Dowty, Director of Action on Rights for Children (Dowty, T, 2011).

DNA profiles will not be taken from children at schools without parental consent. The Bill asserts that if a child refuses to give up any of their biometric information they will not be forced to. Additionally they will not lose out on any opportunities if they refuse to give up their biometric data (HMG, 2010-11: 17). This is a victory for individual choice.



Schools considering extremely intrusive data systems should be deterred. This could be done through requiring schools to request permission from the Information Commissioner's Office (ICO) to hold the data.

Furthermore, as the Bill stands, Schools can disobey the new laws when it comes to permission. With no sanctions, schools who already do not ask for permission have little incentive to comply with the Bill's aims. A sanction could be a fine. This would force schools to see that mass fingerprinting without parental consent is not just morally wrong, but also makes no economic sense.

1j) DNA Retained For National Security

Undoubtedly some DNA has to be retained for national security purposes. Nevertheless, the term national security has broadened since the War on Terror, often into unrelated areas.

A person under suspicion on national security grounds should have rights to appeal to the relevant court, who can act neutrally. The courts could argue that there is no evidence, and thus the DNA cannot be retained. This would increase accountability.

Presently, terrorism-related offences are exempt from the protections outlined in the Bill, as Chief Constables will still be allowed to ask a Magistrate for DNA profiles to be retained indefinitely on national security grounds (HMG, 2010-11: 7). The Government should not undermine liberty when fighting terrorism, as this helps terrorists succeed in destabilising our democracy.

1k) National DNA Database Strategy Board

The creation of a National DNA Database Strategy Board is welcome (HMG, 2010-11: 15). Transparency will be generated, as the body is subject to Parliamentary approval. Finally, it could be a useful monitor of Police Force's actions.

1l) Conclusions

The changes are a start towards the Government promoting liberty, rather than undermining it. However for liberty to be truly safeguarded it needs to go further. If the Governments make the reasonable amendments called for, the relationship between the individual and the state will finally be in favour of the individual.

Chapter 2 : Implications for Surveillance Systems and CCTV

Written by Daniel McMahon

2a) Introduction

“Public acceptance is based on limited and partly inaccurate knowledge of the functions and capabilities of CCTV systems in public places. There may be a need for guidelines that will make possible an informed public acceptance of CCTV through fuller consultation and the provision of information. There is also a need to encourage operational procedures that will maximise the effectiveness of CCTV and minimise any threat to civil liberties which may arise from either sloppy practice or the deliberate misuse of such systems. Any guidelines must anticipate future problems due to the proliferation of CCTV systems, and the pace of technological development which allows increasingly powerful forms of surveillance.”

(Charman, E & Honess, T, 1992: 25):

A Home Office report on the acceptability and effectiveness of CCTV cameras in 1992 foresaw the increasing problems associated with the proliferation of surveillance systems in public areas. It highlighted how surveillance affected the accountability of police, leading to unacceptable levels of intrusion by the state into individual's lives. However, the warnings went unheeded, meaning problems like inadequate Home Office guidelines or statutory controls remain, leading to freedom being attacked. Almost twenty years later, the number of cameras and their scope and power has risen exponentially. New figures suggest there is 1 CCTV camera for approximately every 32 citizens in Britain, with around 1.85 million nationwide (Daily Mail, 2011). Previous estimates have suggested as many as 4.2 million cameras were in operation in Britain (Evening Standard, 2007). The real number probably lies somewhere between the two. British people experience a staggeringly high amount of surveillance compared to other much larger and more authoritarian countries. In 2009, it was calculated that Britain had around 1.5 million more cameras than China and 20% of all global cameras. Simon Davies, Director of Privacy International, said “Britain has established itself as the model state that the Chinese authorities would love to have (Kelly, T, 2009).” The law of government unintended consequences, whereby attempting to solve a problem inadvertently exacerbates the existing problem, has been aptly demonstrated.

The rise of CCTV is sometimes attributed to a reaction to the events of September 11, 2001 and the subsequent War on Terror, but in reality cameras were on the rise well before this as an increasingly first line of attack against crime. In subsequent counter terrorism operations Damian Green believes, “The government sought to clamp down on the entire population instead of concentrating on the tiny number who actively wish us harm. The unintended consequence of this was a surveillance state (Green, D 2010: 45).”

The new Coalition Government is aiming to counter the seemingly inexorable decline of our liberty through the Protection of Freedoms Bill. One subtle yet visible infringement on our privacy has been the rise of the CCTV camera. This report attempts to outline the main themes of the Bill in regard to surveillance systems, what affect it could have, and when necessary, where it could be improved.

2b): The Story So Far

The rise of surveillance camera technology in our communities and on our streets has been silent but deadly as, according to Damian Green MP, “We have steadily and unwittingly turned into a surveillance society’ (Green, D, 2010: 44).” However through the combination of surveillance abuse, research and pressure groups, there has been a growing public consciousness over the issue. Presently, there seems more resistance to wide-scale public surveillance than ever before. Therefore, the Government’s Bill reflects the evolving political and cultural attitudes towards an increasingly watched, yet aware, society.

The number of private cameras is difficult to gauge. However, a 2009 report into the number of local authority controlled CCTV cameras by Big Brother Watch found there were at least 59,753 surveillance cameras operated by the 428 local authorities nationwide. This has risen from around 20,000 eleven years ago. In London alone, there was a minimum of 8,112 public CCTV cameras, which amounted to a rise of 279% in one decade (Big Brother Watch, 2009). This is expensive, as a survey of 366 councils in 2010 highlighted that nearly £315 Million from 2007 was spent on installing and operating CCTV cameras (Greenhill, S, 2010). According to Alex Deane, former director of Big Brother Watch, this has led to ludicrous situations like the Shetland Islands now having more CCTV cameras than the entire San Francisco police department. He also noted, that the numbers calculated by Big Brother Watch are just a fraction of the number of surveillance cameras in operation in Britain (Deane, A, 2010). The extremely large amount of CCTV and ANPR (Automatic Number Plate Recognition) cameras has helped to make the British the most heavily monitored people in the Western world (McKinstry, L, 2010: 166).

Prior to this Bill, local councils and authorities faced minimal regulation on the implementation and usage of CCTV and ANPR surveillance systems. The private sector is of course difficult to administer, but in the public sphere, the industry has grown almost unhindered. Isabella Sankey, Director of Policy at Liberty, has said to the protection of Freedoms Bill Committee “We have seen a sharp increase in the number of CCTV cameras that are up around this country, over the past 10 years in particular. At the same time, we have not seen an increase in regulation (Sankey, I, 2011). “ If you increase the amount of CCTV cameras, allied with no further regulation, then the chances of the cameras being abused are of course augmented.

2c)- Effects On Crime

There is little evidence to suggest that the rise of CCTV has a direct correlation with crime reduction or prevention. As Gill and Spriggs assert after their 2005 report into the effectiveness of CCTV, “CCTV cannot be deemed a success. It has cost a lot of money and it has not produced the anticipated benefits (Gill, M, & Spriggs, A, 2005: 120). Furthermore, a 2009 Metropolitan Police Report found that approximately only one crime was solved per thousand cameras in Britain. When hearing this David Davis, former Shadow Home Secretary said, “It should provoke a long overdue rethink on where the crime prevention budget is being spent (BBC, 2009).”



A Home Office report in 2005 explored the impact of CCTV on crime and the fear of crime in different areas (city outskirts, market town, estate etc). It concluded that out of the 14 areas studied, only two schemes experienced a statistically significant reduction in recorded crime relative to the control area (Gill, M & Spriggs A, et al, 2005: 34).

2d)- State Surveillance Going Wrong

One example of the potential for state surveillance to go awry was the experiences of Sparkbrook and Washwood Heath, two predominantly Muslim neighbourhoods in Birmingham. A network of over 200 CCTV and ANPR cameras was set up in a rapid time period, marketed to locals as a general crime prevention measure. However, it emerged that the surveillance network was being financed under a secretive counter-terrorism initiative known as Project Champion. The underhand tactics and opaque nature of the events in Birmingham sparked anger amongst civil liberties groups and within the local community. This anger is presumably on two counts, firstly that it was set up with no public consultation and secondly, it seemingly demonstrated rather obvious racial profiling of an overtly Muslim community. The police belatedly realised this when West Midlands Police Chief Constable, Chris Sims, admitted “He was 'deeply sorry' that his force got the balance between counter-terrorism and intrusion into people's lives so wrong (Birmingham Post, 2010).”

A recent case in Edinburgh of a female cleaner being stalked by a security guard, further exemplifies the potential for surveillance to be perverted. The security guard in question James Tuff, used the camera system at Dynamic Earth to track his victim and then radio her with lewd comments. He eventually sexually assaulted Dora Alves inside the attraction, which has 500,000 visitors a year (Lavelle, C, 2011). It is reports like this, and other examples of overbearing and intrusive surveillance allowed under the Regulation of Investigatory Powers act 2000 that make the proposed changes in the Bill very welcome.

2e) Government Changes

Part II of the Protection of Freedoms Bill deals with the regulation of surveillance, CCTV, ANPR and other surveillance camera technology. There will be a number of changes implemented to better regulate surveillance technology. This is important as according to Isabella Sankey, whatever the real number of cameras in operation today in Britain, the number is somewhat irrelevant, what is required is “proper legal regulation and proportional use (Daily Mail, 2011).”

Two specific changes proposed in the Bill stand out. First, is the creation of a statutory code of conduct, which will provide guidelines for local councils and police authorities wishing to implement a surveillance network in a community. Secondly, there will be the creation of a Surveillance Camera Commissioner who will oversee the state of CCTV and liaise with the Secretary of State and other authorities to ensure surveillance potential is not abused. The report will now look at these developments in more detail.

2f) the Statutory Code Of Conduct

The existing Secretary of State will be in charge of creating the code of practice containing guidance about surveillance camera systems (Her Majesty's Government (HMG), 2010-11: 19).

The code of conduct specified in clause 29 will offer extensive guidance to local authorities when planning to set up a surveillance system. A thorough assessment will be required. Aspects to consider include the location of camera apparatus, the type of surveillance apparatus to use, the cost and value, and ultimately whether or not the surveillance system is worth implementing. Only when these different factors are taken into consideration should there be a decision to continue or not. The code will also contain information on the consultation and complaints procedures. It also rules on what can and cannot be utilised by virtue of obtaining image information (Almandras, S, 2011: 16). These are encouraging steps.

The code must pass through both Houses of Parliament, and the draft may be altered if either House makes any amendments. Importantly, the Secretary of State will be obliged to keep the surveillance camera code under review (HMG, 2010-11: 21). Hopefully, this will prevent the executive ignoring the legislature's concerns. Despite no obvious attempts to tackle the increasing sophistication of intelligence surveillance, this will mean the code does not remain in a state of perpetual stagnation or forgotten about. Under the new provisions, the Home Secretary will have to consult with several authorities, named in the Bill, when devising the code. They include the new Surveillance Camera Commissioner, the Information Commissioner, the Association of Chief Police Officers and any other party, which the Secretary deems appropriate. This will ensure the Home Secretary has a relatively wide breadth of advice and feedback.

The new code will force the police and local councils who want to implement a CCTV system to be more transparent in their approach and to offer details before being cleared to introduce it. Under Clause 32, it is obliged that the code is made publicly available for any seeking its details and guidelines. This should encourage a move away from the existing opaque modus operandi (HMG, 2010-11: 20).

It is wrong that surveillance cameras have been used without a proper regulatory framework, which is why the Bill's emphasis on the new statutory code is a welcome development that could be extended or strengthened in the future.

2g) the Surveillance Camera Commissioner

The Bill also allows for the appointment of a Surveillance Camera Commissioner who will be responsible for "encouraging compliance with the code of practice, reviewing its operation and providing advice on it, including on any changes that might be necessary (May, T, 2011). "

The Commissioner will be responsible for monitoring the usage of the code, and encouraging compliance with the code, reviewing the operation of the code and providing

advice about the code (including changes to it or breaches of it) (Almandras, S, 2011: 18). Essentially, the Commissioner acts as a sober interloper, providing constructive advice on the guidelines proposed.

Furthermore, there will be certain standards applicable to persons using or maintaining systems or apparatus as well as the persons processing information obtained by virtue of systems (HMG, 2010-11: 20). This could force people to think twice before using these surveillance powers. Additionally, the new code will suggest the length of time certain data should be retained. This will be particularly important when dealing with data gained from ANPR cameras, which the Home Office admits is more easily searchable (Independent, 2011). It is fundamental that data should not be held for any longer than necessary.

Under the new rules, local councils and police authorities intending to introduce CCTV systems in their communities will have to justify their choices to the public. Any person seeking to investigate or gain information on surveillance camera systems in their community will be able to obtain that information easily and readily whilst the personal data itself is appropriately safeguarded (Almandras, S, 2011: 17). It is hoped that through this, public knowledge of the statistics and objectives of will increase, as will public confidence in the proportionate and correct use of surveillance technology.

2h) Future Implications and Suggested Improvements

The Bill has brought the topics surrounding surveillance systems and what type of society we desire to live in, to the forefront of national and Parliamentary debate. This can only be positive.

While the new legislation will control CCTV and ANPR more tightly, there are still concerns that the pace of technological change will outpace legislative updates. The potential of sophisticated technology to improve the scope, versatility and accuracy of visual monitoring is extensive. For example, in 'event-led' motion cameras, body language sensors can detect 'unusual movement' at train or tube stations. This technological advancement will make it harder for the state's apparatus to give up its surveillance addiction. It is apparent that the surveillance code of conduct will have to evolve with the technology or face being left inadequate. Therefore it needs to be held under regular review, but how regularly this will occur is not emphasised clearly in the Bill. Thus, an amendment should be inserted, calling for yearly reviews of the code of conduct. It is surprising that, despite the relatively clear direction that 'intelligent' technology is moving, the Government did not pre-empt this.

The code of practice for surveillance systems has included provisions for several functions. It will contain considerations surrounding location, types of apparatus, utility and feasibility of the system, as well as publication of relevant information and standards applying to those handling the data. Nevertheless, it is deeply concerning that, according to Liberty, "The Bill does not make the provision of guidance in these areas compulsory (Farthing, S, & Robinson, R & Sankey, I, 2011: 12)." The guidance should certainly be made compulsory or risk discouraging those whom the guidance is aimed at, namely local councils and the police authorities; after all, making something compulsory means forcing people to do

what they otherwise might not do. For instance, it is highly likely that if taxation were not compulsory most people would avoid it.

Similarly, it is regrettable that in outlining the effect of the code, Clause 33(2) does not include the potential for liability when contravening the surveillance camera code:

“A failure on the part of any person to act in accordance with any provision of the surveillance camera code *does not of itself make that person liable to criminal or civil proceedings.*” (HMG, 2010-11: 22) [emphasis my own]

Despite the Bill suggesting that the guidelines may include provisions on which locations would be suitable and which would not, coercive requirements to fully abide by the advice are strangely lacking. The Bill should therefore underscore, through tougher language, punishments for breaking the new code. This could have a profound effect in dissuading individuals from paying minimal attention to it. If there is not any punishment mechanism, people like in the Edinburgh case will get away with abusing surveillance powers. Also, it could mean that officials using surveillance powers will still be unaccountable for their actions.

2i) Conclusions

In the difficult economic climate, the effectiveness and spiralling costs of profligate CCTV usage have to come under scrutiny. The value of surveillance systems when compared to conventional methods of crime prevention needs to be questioned openly. With most departments facing expenditure cuts, it is correct that the Government is acknowledging the spiralling costs of CCTV surveillance. Whilst there are some benefits, the matter should be viewed like any business would view a balance sheet. Currently, the liabilities heavily outweigh the profits of an increasingly spied upon population, because of the financial implications, intrusiveness and negligible effect on reducing crime.

Moreover, CCTV can dissuade local communities and citizens from taking action themselves, as they become dependent on the state, sapping them of responsibility. As Philip Johnston has contended, “When the state seeks to do everything, its citizens feel they need do nothing. Big government removes the obligation on its citizens of independent action, self-sacrifice and voluntary effort (Johnston, P, 2010: 80).” The Bill will make it more difficult for local councils and police authorities to implement surveillance as whimsically as they have done. This will create an atmosphere where people will have consider and question the profligate spread of CCTV cameras in certain areas, as a direct replacement for police officers, who are not merely neutral bystanders. This could help reduce crime as, since the growth of CCTV, the primary means of crime prevention, more traditional, community based measures have too often been discarded in recent years (Privacy International, 1997) However, despite assurances of tighter regulation and less CCTV profligacy, the fundamental reality remains that CCTV camera usage is still increasing and will continue to do so, only perhaps not as fast. Unfortunately, we may not see an end to abuse of surveillance powers yet, despite this first, encouraging step.



The Coalition Government has set out its stall in defence of civil liberties and against the tide of the surveillance state. It needs to be bolder though to slay the dragon of the Big Brother state.



Chapter 3: Implications for the Regulation of Investigatory Powers Act 2000 (RIPA)

Written By Devin Knox

3a) Introduction

The new Protection of Freedoms Bill is attempting to make many positive changes to RIPA. This Act was designed to regulate the power of public bodies carrying out surveillance and investigation operations and covers the interception of communication. It tried to deal with the ever-changing means of communication, but many think civil liberty concerns were ignored. It also endeavoured to prevent or detect serious crimes, thus safeguarding the economic well being of the UK. The Act could be used for a wide range of security issues. After all, there are not many Acts of Parliament that end up being used for both snooping in bins and supposedly top-secret terrorist operations.

3b)-Interception of Communications

RIPA allows for the interception of communications by the Home Secretary, which is fraught with concerns about undermining individual freedom. In 2009, the Secretary of State issued 1514 interception warrants to access telephone or private email conversations (Liberty, 2010: 1). It was a case of the Home Secretary literally invading individual privacy, sometimes on mistaken or circumstantial evidence. Clearly there was little respect paid to the idea of individual privacy, which is necessary if the ideal of innocent until proven guilty remains. This provision can now be carried out by numerous bodies, which include: the Security Service (MI5), the Secret Intelligence Service (MI6), Government Communication Headquarters (GCHQ), Serious Organised Crime Agency (SOCA), police forces, and competent authorities of overseas countries (Liberty, 2010: 4). Privacy campaigners believe there are many more organisations that have access to these powers under the law (Guardian, 2009). This is quite different to the intention of the Bill, where only nine organisations including the police and security services were allowed to use these powers. This shows that when governments get powers, they inevitably try to extend it to as many public bodies as possible.

Furthermore, in 2010 alone 134 authorities made 1,811 requests, which was a slight increase on the previous year, where figures were in the region of 1,700. In general every year since these surveillance powers have been in place the numbers have increased. So rather than regulating surveillance as the legislation suggests it in fact seems to have encouraged surveillance. What is even more disturbing is that the present Intercept of Communications Commissioner who revealed these figures to the Protection of Freedoms Public Bill Committee, thinks that this number if anything is too low, and that authorities should use their powers more often (Kennedy, P, 2011).

These powers can easily threaten freedom of speech. For example, a person expressing their political views in private could be spied on by the Government, which can act against this person. Whilst freedom of speech being undermined catastrophically in this way seems unlikely in modern day Britain, when the state has powers like these, they generally use them. For example, in 2007 alone there were 519,260 requisitions for communications



data from telephone companies and ISPs. Whilst the content of an email or telephone call can only be obtained with a warrant from the Home Secretary, RIPA does allow government to access communications data for a wide range of reasons including national security and tax collection (Freedom House, 2009: 111). This figure went on an upward trajectory in 2008 to 525,130 requests (Liberty, 2010: 3). Privacy concerns here are perfectly valid, if you look at Government departments' record of looking after personal data.

3c) Surveillance of Private Property

RIPA allows for covert filming or bugging someone's home or vehicle so your private vehicle or home effectively becomes the property of the state. This power is not used sparingly as in 2009-2010 there were 384 of these warrants issued (Liberty, 2010: 1). It is a fearful thought that Big Brother can listen to conversations in your private residence. No person should be put under suspicion by an authoritarian state in their home.

3d) Monitoring In Public Places

RIPA has allowed authorities to covertly monitor the movement of individuals in public places. They can be follow them around, film them, or track them audibly. In fact, in 2009-2010, law enforcement officers issued 15,285 of these directed surveillance authorisations and other public authorities received 8,477 (Liberty, 2010: 2). Those authorised to use this provision include: the police, SOCA, the intelligence services, HMRC, government departments, all local authorities, fire authorities, the Charity Commission, the Environment Agency, the Financial Services Authority, the Food Standards Agency, the Gambling Commission, the Office of Fair Trading, the Gang masters Licensing Authority, the Care Quality Commission, the Health and Safety Executive, NHS bodies, the Inspector of Education, the Information Commissioner and Royal Pharmaceutical Society.(Liberty, 2010: 8) While surveillance is necessary at times to prevent crime and other unsocial behaviour, the numbers issued demonstrate that it is being used disproportionately. A citizen should not be subjected to this type of surveillance without proper reason and cause yet, with large numbers like this, it would be unsurprising to come across miscarriages of justice. Why does the Food Standards Agency need to monitor public places. Are they going to use these powers to monitor what people eat, and if they are doing so, why do they need to?

3e) Covert Intelligence

RIPA provides a provision allowing for Covert Human Intelligence Services. This provision allows for an agent to make contact and maintain a relationship with a person covertly to gather information. This provision was used 5,320 times by law enforcement authorities and 229 times by other public authorities in 2009-2010. The provision can be used by the same bodies mentioned above (Liberty, 2010: 10). A person should not have to live in fear that an acquaintance may actually be someone sent to spy on them. This could lead a person to self-incriminating himself. Moreover, it will lead to people distrusting the state.

3f) Communications Monitoring

The last provision of RIPA allows authorities to examine a person's communication record. This does not include the substance of the communication but allows authorities to see where a phone call was made or which website was visited, the date and time of communication and how long it lasted, and subscriber information. The allowed authorities include amongst others the Serious Fraud Office, the Royal Mail Group, IPCC (Independent Police Complaints Commission), and the Pensions Regulator (Liberty, 2010: 12).

3g) Effects On the Innocent

Those who were put under surveillance and found innocent were not notified of this. This lack of accountability allowed RIPA to become a snooper's charter. If there had been a provision in place notifying when innocent people had been spied upon, it would have encouraged the state's apparatus to investigate by conventional means and think twice about using RIPA powers, because they would fear being embarrassed and punished for unfairly targeting innocent individuals. However, just as with the DNA database and CCTV surveillance, many innocent people became victims of injustice.

3h) Investigatory Powers Tribunal (IPT)

The original RIPA legislation did set up the IPT to investigate anything done by an organisation to a person under RIPA. It could also investigate complaints about alleged conduct by or on behalf of intelligence services. However, the IPT was designed as a secret charter and there was no right of appeal and the hearings all had to be in private. The secretiveness and the lack of an appellate process go against common judicial principle. Between 2000 and 2009 the IPT looked into 956 complaints and only found fault 4 times (Chalmer, S, 2010:). It seems that the IPT was ineffective in regulating RIPA.

3i) Intrusion Levels

The powers held under RIPA have led to a shocking level of intrusion by the state. Campaign groups have discovered that 12,500 are under surveillance every year and never know. There is no public accountability, as people do not know that they are being spied upon. Under RIPA legislation 14,000 spying operations are conducted by councils, police and other bodies (Chalmers, S, 2010). It seems that the state is more interested on intruding into people's lives than looking after them.

3j) Local Councils

In some instances organisations such as MI5 or MI6 require the power to use covert surveillance to protect national security, but is it really necessary for local councils to spy on their citizens to such a large extent? Local councils were some of the worst offenders for using RIPA surveillance with 372 local councils using RIPA 8,575 times over the past two years, meaning an average of eleven surveillance operations each day. This surveillance only resulted in 399 prosecutions. (Big Brother Watch, 2010: 5) The lack of prosecution could mean that the surveillance was being used for things other than to detect crime and

is a massive waste of resources as it was not an effective crime-fighting tool. Newcastle-Upon-Tyne Council can call themselves leaders in this field after using RIPA to spy on their residents 231 times in 2 years (Appleyard, N, 2010). Obviously, Newcastle is wasting a large amount of its resources when they could be used to strengthen the community, rather than treating everyone in the community as a potential criminal.

Councils have also used their powers for reasons not altogether altruistic. For instance, in June 2008, 121 local councils revealed that they had used the legislation in a 12-month period to monitor behaviour by examining the private communications of residents (Guardian, 2009). One example of this was the actions of Poole Borough Council who spied on Tim Joyce, Jenny Paton and their children to see if they were cheating the school catchment system. The level of intrusion included obtaining phone billing records and tracking her and her children's travel for 3 weeks. Moreover, they admitted the powers supposedly only to track criminals and terrorists were used six times (BBC, 2008). This is an example of the powers being used disproportionately, ridiculously and intrusively due to a complete lack of regulation. Jenny Paton fought a legal battle with Poole Council claiming what they did was illegal and the IPT ruled in her favour ruling unanimously that it was illegal. (Chalmers, S, 2010).

Additionally, RIPA has been used by councils to spy on their employees. For example, Darlington Council was particularly proficient in spying on their own employees whom they suspecting were lying about their car parking. It seems the common sense approach of talking to your own employees has gone out of the window. Five councils became part of the army of the nanny state policing lifestyle choices by spying on people who they suspect of breaking the smoking ban. In perhaps one of the clearest examples, Suffolk County Council used RIPA powers to make a "test purchase" of a puppy. I'm sure that the people of Suffolk are happy that their hard earned money is being wasted on causes like this. The powers have been also been used to monitor work time, sick pay, and even to spy on their wardens who are employed to spot crime (Appleyard, N, 2010). If private companies acted like this, it would be considered an extreme invasion of privacy and could result in litigation. Those employed by the council should uphold the same standards. Additionally, it is an abuse of power. That they are being used in this way suggests the powers should be regulated tightly or removed completely.

Brian Binley MP proposed this in 2008, after Northampton Borough Council was found to have used powers meant for counter-terrorism operations to catch people who let their dog foul on the grass. He said, "As I understand it, what is happening is that somebody is naming a dog owner whose dog is defecating on the pavement and the dog owner is not picking it up. So what the borough of Northampton does is go out with a secret camera. I just find this remarkable. If it was not so serious it would be totally laughable. But we really are turning local authorities into private detectives or the equivalent of KGB operatives. I just wonder whether the people in this country want this world or not - I suspect they do not (Binley, B, 2008)."

The sad fact is that many citizens have been spied upon by their local councils without even knowing it. It is excellent that Jenny Paton was able to win her legal battle but innocent people should be informed of surveillance and able to take the guilty authority to "court"

and gain some sort of compensation (The Freedom Association, 2010). Additionally, if a crime is a serious offence it is more than appropriate that the police should investigate it. Local councils will still be able to catch people committing these crimes by employing wardens and putting more police on the beat.

3k) What the Government's Bill Aims To Do:

The Home Secretary realised that the present situation could not be allowed to continue. She pointed out that "school catchment area rules and dog fouling are not offences that warrant being subject to surveillance. These tactics are more appropriately used for tackling serious crime and terrorism, and it was irresponsible of the previous Labour Government not to put in place stronger safeguards for their use (May, T, 2011)." The new Freedom Bill adds a provision that requires a magistrate to give approval to an authorised person before acquiring communications data (HMG, 2010-11: 24-25). We hope this provision will stop the frivolous use of RIPA powers.

It also aims to prevent councils from using RIPA powers for anything other than prevention of a serious crime. (HMG, 2010-11: 24-25). A magistrate is a much better form of authorisation than the original form of self-authorisation for many reasons. A magistrate has objectivity and can look at the evidence presented and decide if the reasoning for the warrants merits approval. They do not have the self-interest that the body seeking to carry out the investigation does and therefore they will make the system less open to abuse.

The Home Secretary has also said, "Local authorities will be authorised to use directed surveillance only for offences that carry a maximum custodial sentence of at least six months." Subject to limited exemptions relating to the under-age sale of alcohol and tobacco, this measure will restrict local authorities' use of surveillance to serious cases (May, T, 2011)."

Communications data regulation through a voluntary code of conduct under the Anti-Terrorism, Crime and Security Act 2001 includes 3 main areas:

- ⤴ Traffic Data: This says where a person was when a mobile phone call, Internet connection or some other means of communication took place.
- ⤴ Service Use: tells how communication occurred, the date and time it happened, and how long it lasted.
- ⤴ Subscriber Information: The name and address and details of direct debit of people using communication means.
- ⤴ The conditions for approval remain the same as before. It will still be used for the protection of national security, preventing serious crimes, and protecting the economic well-being of the United Kingdom which includes collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department. Approval will be granted only if the judicial authority believes that there are reasonable grounds to do so and that obtaining communications is necessary and reasonable to achieve one of the aims mentioned earlier (Home Office, 2001: 4).



Hopefully these welcome changes will mean that the vast majority of the public can go about their business without the threat of being spied upon. It should also represent a victory for freedom of speech, as the regulation should act as a check on the Government monitoring people's political opinions.

3l) Suggestions

Whilst giving power to magistrates is a move in the right direction, the generality of the phrase serious crime presents a problem. With no specific guidelines, a magistrate will be forced to decide if the offence is bad enough to grant a local council a warrant and this personal decision may result in discrepancy in warrants granted. The vagueness of the instruction given to a magistrate does not clearly mark out what is "responsible" to issue a RIPA warrant. This should be plainly set out in a codified way so as not to be abused by judges and be equal for everyone under the law.

Additionally, clearer instructions will reduce the likelihood for the state apparatus to be able to abuse surveillance powers. By doing this, it would mean what has been allowed to be authorised by public authorities can only be authorised by the judiciary, which will bring in concerns about human rights as well as having an approach which will be much more independent. If this does not happen, we may see more stories of RIPA surveillance power being abused by public authorities. However if the Bill is strengthened it will go the full way down the checks and balances route, which will mean a much more proportionate and fair use of the powers. This would provide the necessary reassurance that the public needs.

We also think that presently the Bill still allows police and intelligence services, to abuse their powers. This is because both these bodies will be exempt from judicial authorisation as the Bill stands (Metcalf, E, 2011). As RIPA covers areas, for example intercepting phone calls and bugging people's home that intrudes into a person's privacy, this needs to be policed properly. Therefore both these bodies should also be under judicial authorisation. If not both these bodies will continue abusing their powers.

We are also worried that unnecessary exemptions are being made. For example, Mrs. May's stated that local authorities can still carry out direct surveillance operations in relation to under age tobacco and alcohol sales. This is a minor crime, which should be treated like other minor crimes in the Bill and thus not lead to unnecessary surveillance.

3m) Conclusions

These proposals to change RIPA are an excellent start and should provide more personal privacy to everyone across the nation. However, the Bill does not go far enough and could be changed to offer more protection to citizens from being spied upon. Even with the bill, RIPA powers are still intrusive and could still be used by people who are trained for covert surveillance. With some worthwhile changes to the Bill, this unsatisfactory situation can end.



BIBLIOGRAPHY

Section 1: The DNA Database and Biometric Data Taken From Children

Almandras, S, (2010). Retention of Fingerprint and DNA Data. [online]. [accessed 6th March 2011]. Available From:

<http://www.parliament.uk/briefingpapers/commons/lib/research/briefings/snha-04049.pdf>

Blackwood, N, (2011). Second Reading of Protection of Freedoms Bill. [online]. [accessed 7th March 2011]. Available From:

<http://www.publications.parliament.uk/pa/cm201011/cmhansrd/cm110301/debtext/110301-0003.htm>

Brake, T, (2011). Second Reading of Protection of Freedoms Bill. [online]. [accessed 7th March 2011]. Available From:

<http://www.publications.parliament.uk/pa/cm201011/cmhansrd/cm110301/debtext/110301-0003.htm>

Chishti, R, (2011). Second Reading of Protections of Freedoms Bill. [Online]. [Accessed 7th March 2011]. Available From:

<http://www.publications.parliament.uk/pa/cm201011/cmhansrd/cm110301/debtext/110301-0003.htm>

Copper, W, (2010). The Real DNA Database Dividing Line. [online]. [accessed 6th March 2011]. Available From:

<http://www.guardian.co.uk/commentisfree/libertycentral/2010/apr/16/dna-database-dividing-line>

Cunningham, T,(2006). Arrested and DNA Tested for Jokingly Pinging a Bra. [online] .[accessed 2nd March 2011]. Available From: <http://www.dailymail.co.uk/news/article-398002/Arrested-DNA-tested--jokingly-pinging-bra.html>

Derbyshire Constabulary, (2010). DNA Database and Samples .[online]. [accessed 3rd March 2011]. Available From: <http://www.derbyshire.police.uk/About-us/Freedom-of-Information/Lists-and-Registers/FOI-Disclosure-Logs/Organisational-Information/2010/DNADatabaseandSamples.aspx>

Daily Mail, (2006) Grandmother Arrested for Stealing football for Revenge. [online]. [accessed 2nd March 2011]. Available From: <http://www.dailymail.co.uk/news/article-408819/Grandmother-arrested-stealing-football-revenge.html>



Dowty, T, (2011). Protection of Freedoms Bill Committee 22nd March: Afternoon. [online]. [accessed 23rd March]. Available From: <http://www.publications.parliament.uk/pa/cm201011/cmpublic/protection/110322/pm/110322s01.htm>

Floru, J, (2011). Will the Freedom Bill Actually Retain the Database of the Innocents .[online]. [accessed 29th March 2011]. Available From: <http://conservativehome.blogs.com/platform/2011/03/freedom-bill-to-retain-the-database-of-the-innocents.html>

Genewatch UK, (2005). Memorandum by Genewatch UK [online]. [accessed 7th March 2011]. [online]. Available From: <http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/8013002.htm>

Genewatch UK,(2010). Memorandum Submitted by Genewatch UK (CR02). [online]. [accessed 7th March 2011]. Available From: <http://www.publications.parliament.uk/pa/cm200910/cmpublic/crimeandsecurity/memos/uCCR0202.htm>

Genewatch UK,(2010). Facts and Figures. [online]. [accessed 4th March 2011]. Available From: <http://www.genewatch.org/sub-539481>

Genewatch UK,(2011). Protection of Freedoms Bill. [online]. [accessed 10th March 2011]. Available From: <http://www.genewatch.org/sub-566498>

Glen, J, (2011). Second Reading of Protection of Freedoms Bill. [online]. [accessed 7th March 2011]. Available From: <http://www.publications.parliament.uk/pa/cm201011/cmhansrd/cm110301/debtext/110301-0003.htm>

Her Majesty's Government Protection of Freedom Bill, (2010-11). [online]. [accessed 28th February 2011]. Available From: <http://services.parliament.uk/bills/2010-11/protectionoffreedoms.html>

Johnson, G, (2011). Second Reading of Protections of Freedoms Bill. [online]. [Accessed 7th March 2011]. Available From: <http://www.publications.parliament.uk/pa/cm201011/cmhansrd/cm110301/debtext/110301-0003.htm>

Lewis, J, (2010). Detectives Trawl DNA Database 60 times a year-Hunting for Criminals' Relatives. [online]. [accessed 5th March 2011]. Available From: <http://www.dailymail.co.uk/news/article-1254354/Detectives-trawl-DNA-database-60-times-year--hunting-criminals-relatives.html>



May, T, (2011). Second Reading of Protection of Freedoms Bill . [online]. [accessed 7th March 2011]. Available From:

<http://www.publications.parliament.uk/pa/cm201011/cmhansrd/cm110301/debtext/110301-0003.htm>

NPIA(2010). Statistics [online]. [accessed 4th March 2011]. Available From:

<http://www.npia.police.uk/en/13338.htm>

Pugh, G, (2011). Protection of Freedoms Bill Committee: Tuesday 22nd March-Morning . [online]. [accessed 23rd March 2011]. Available From:

<http://www.publications.parliament.uk/pa/cm201011/cmpublic/protection/110322/am/110322s01.htm>

Shannon, J, (2010). Second Reading of Protections of Freedoms Bill. [online]. [Accessed March 7th 2011]. Available From:

<http://www.publications.parliament.uk/pa/cm201011/cmhansrd/cm110301/debtext/110301-0003.htm>

Wallace, H, (2006). The UK National DNA Database: Balancing Crime Detection, Human Rights and Privacy. [Online]. [accessed 7th March 2011]. Available From:

<http://www.nature.com/embor/journal/v7/n1s/full/7400727.html>

Whitehead, T, (2009). More than one in 10 people on DNA Database for First Time. [online]. [accessed 6th March 2011]. Available From:

<http://www.telegraph.co.uk/news/uknews/law-and-order/6448452/More-than-one-in-10-people-on-DNA-database-for-first-time.html>

Section 2: Implications For Surveillance Systems And CCTV

Almandras, S, (2011). Protection of Freedoms Bill Research Paper. [online]. [accessed 15th March 2011]. Available From:

<http://www.parliament.uk/briefingpapers/commons/lib/research/rp2011/RP11-020.pdf>

BBC, (2009). 1,000 Cameras Solve One Crime. [online]. [accessed 1st March 2011]. Available From: <http://news.bbc.co.uk/1/hi/8219022.stm>

Big Brother Watch, (2009). Big Brother is Watching: Local Council Controlled CCTV Cameras Treble in a Decade. [online]. [accessed 28th February 2011]. Available From:

<http://www.bigbrotherwatch.org.uk/home/2009/12/big-brother-is-watching-local-council-controlled-cctv-cameras-treble-in-a-decade.html>

Birmingham Post, (2010). Police Chief deeply sorry over Birmingham Anti-Terror Spy Cameras. [online]. [accessed 28th February 2011]. Available From:

<http://www.birminghampost.net/news/2010/09/30/police-chief-deeply-sorry-over-birmingham-anti-terror-spy-cameras-65233-27375456/>



Charman E & Honess, T, (1992). Closed Circuit Television in Public Places: Its Acceptability and Perceived Effectiveness. [online]. [accessed 1st March 2011]. Available From: <http://rds.homeoffice.gov.uk/rds/prgpdfs/fcpu35.pdf>

Daily Mail (2011). Big Brother is Definitely Watching you. [online]. [accessed 4th March 2011]. Available From: <http://www.dailymail.co.uk/news/article-1362493/One-CCTV-camera-32-people-Big-Brother-Britain.html>

Deane, A, (2010). Facts About CCTV Cameras. [online]. [accessed 3rd March 2011]. Available From: <http://futureoftheconservativeparty.blogspot.com/2010/06/facts-about-cctv-cameras.html>

Evening Standard (2007). George Orwell, Big Brother is Watching your House. [online]. [accessed 26th February 2011]. Available From: <http://www.thisislondon.co.uk/news/article-23391081-george-orwell-big-brother-is-watching-your-house.do>

Gill, M & Spriggs, A, (2005). Home Office Research Study 1992: Assessing the Impact of CCTV. [online]. [accessed 27th February 2011]. Available From: <http://rds.homeoffice.gov.uk/rds/pdfs05/hors292.pdf>

Gill M & Spriggs A, et al, (2005). The Impact of CCTV: Fourteen Case Studies. [online]. [accessed 27th February 2011]. Available From: <http://rds.homeoffice.gov.uk/rds/pdfs05/rdsolr1505.pdf>

Green, D(2010). Freedom is a One Nation Issue. In: Deane, A, ed. Big Brother Watch: The State of Civil Liberties in Modern Britain. pp.44-53

Greenhill, S (2010). Big Brother Town Halls Squander £315m on CCTV despite Massive Job Cuts. [online]. [accessed 2nd March 2011]. Available From: <http://www.dailymail.co.uk/news/article-1342010/Town-halls-squander-315m-CCTV-years-despite-massive-job-cuts.html#ixzz1A43KasgY>

Her Majesty's Government Protection of Freedom Bill, (2010-11). [online]. [accessed 5th March 2011]. Available From: http://www.publications.parliament.uk/pa/bills/cbill/2010-2011/0146/cbill_2010-20110146_en_1.htm

Independent, (2011). New Code to Govern CCTV Cameras. [online]. [accessed 4th March 2011]. Available From: <http://www.independent.co.uk/news/uk/crime/new-code-to-govern-cctv-cameras-2229268.html>

Johnston, P, (2010). Freedom and Liberty Under the Coalition. In: Deane A, ed. Big Brother Watch: The State of Civil Liberties in Modern Britain. pp.76-80

Kelly, T, (2009). Revealed: Big Brother Britain has more CCTV Cameras than China. [online]. [accessed 4th March 2011]. Available From: <http://www.dailymail.co.uk/news/article-1205607/Shock-figures-reveal-Britain-CCTV-camera-14-people--China.html>



Lavelle, C, (2011). Security Guard used CCTV System to Stalk Cleaner. [online]. [accessed 17th March 2011]. Available From: <http://www.heraldscotland.com/news/home-news/security-guard-used-cctv-system-to-stalk-cleaner-1.1090438>

May, T, (2011). Protection of Freedoms Bill 2010-11 Second Reading. [online]. [accessed 4th March 2011]. Available From: <http://www.theyworkforyou.com/debates/?id=2011-03-01a.205.0&s=speaker%3A10426#g219.3>

McKinstry, L, (2010). A Land of Liberty?. In: Deane, A, ed. Big Brother Watch: The State of Civil Liberties in Modern Britain. pp.163-173

Privacy International,(1997). CCTV Frequently Asked Questions. [online]. [accessed 4th March]. Available From: <https://www.privacyinternational.org/article/cctv-frequently-asked-questions#3>

Sankey, I, (2011). Protection of Freedoms Bill Public Bill Committee: 22nd March- Afternoon. [online]. [accessed 22nd March 2011]. Available From: <http://www.publications.parliament.uk/pa/cm/cmtoday/cmstand/output//110322p-01.htm>

Section 3: Implications For the Regulation of Investigatory Powers Act

Appleyard, N, (2010). Survey Highlights Council Surveillance Offenders. [online]. [accessed 14th March 2011]. Available From: <http://www.localgov.co.uk/index.cfm?method=news.detail&id=89059>

BBC, (2008). Council Admits Spying on Family. [online]. [Accessed 17th March 2011]. Available From: <http://news.bbc.co.uk/1/hi/england/dorset/7341179.stm>

BBC, (2008). Family's Shock at Council Spying .[online]. [accessed 17th March 2011]. Available From: <http://news.bbc.co.uk/1/hi/england/dorset/7343445.stm>

Big Brother Watch, (2010) The Grim RIPA: Cataloguing the ways in which local authorities have abused their covert surveillance power. [online]. [accessed 14th March 2011]. Available From: <http://www.bigbrotherwatch.org.uk/TheGrimRIPA.pdf>

Binley, B, (2008). MP Calls for Councils to stop Using Anti-Terror Laws. [online]. [accessed 13th March 2011]. Available From: http://www.northamptonchron.co.uk/news/local/mp_calls_for_councils_to_stop_using_anti_terror_laws_1_926776

Chalmers, S, (2010). Meet the Family who Beat Big Brother: But after stopping Council Spies, Their Children still ask, are those Nasty Men Following us. [online]. [accessed 17th March 2011]. Available From: <http://www.dailymail.co.uk/news/article-1300965/Meet-family-beat-Big-Brother-But-stopping-council-spying-children-ask-nasty-men-following-us.html>



Freedom House, (2009). Freedom on the Net: A Global Assessment of Internet and Digital Media. [online]. [accessed 16th March 2011]. Available From: <http://www.freedomhouse.org/uploads/FreedomOnTheNet.pdf>

Guardian, (2009). Regulation of Investigatory Powers Act 2000. [online]. [accessed 15th March 2011]. Available From: <http://www.guardian.co.uk/commentisfree/libertycentral/2009/jan/14/regulation-investigatory-powers-act>

Her Majesty's Government Protection of Freedom Bill, (2010-11).[online]. [accessed 13th March 2011]. [Available From: http://www.publications.parliament.uk/pa/bills/cbill/2010-2011/0146/cbill_2010-20110146_en_1.htm

Home Office, (2001). Retentions of Communications Data Under Part 11: Anti Terrorism, Code and Security Act 2001 Voluntary Code of practice. [online]. [accessed 13th March 2011]. Available From: <https://www.legislation.hms.gov.uk/si/si2003/draft/5b.pdf>

Kennedy, P, (2011). Protection of Freedoms Bill Public Bill Committee 22nd March- Morning: [accessed 23rd March]. [online]. Available From: <http://www.publications.parliament.uk/pa/cm201011/cmpublic/protection/110322/am/110322s01.htm>

Liberty, (2010). Summary of Surveillance Powers Under RIPA Available: [online]. [accessed 15th March]. Available From: <http://www.liberty-human-rights.org.uk/policy/reports/introduction-to-ripa-august-2010.pdf>

May, T, (2011). Protection of Freedoms Bill Second Reading debate. [online]. [Accessed 16th March]. Available From: <http://www.theyworkforyou.com/debates/?id=2011-03-01a.205.0&m=40584>

Metcalfe, E, (2011). Protection of Freedoms Bill Public Bill Committee 22nd March- Afternoon. [online]. [accessed 23rd March]. Available From: <http://www.publications.parliament.uk/pa/cm201011/cmpublic/protection/110322/pm/110322s01.htm>

The Freedom Association, (2010). RIPA legislation used by Council to Spy on Family. [online]. [Accessed: 13th March] Available: http://www.tfa.net/the_freedom_association/2010/08/ripa-legislation-used-by-council-to-spy-on-family.html