## CONTENTS

**INTRODUCTION** ........................................................................................................... 1

**ABOUT THE MANIFESTO** .......................................................................................... 2

---

**PART 1**

**THE 2010 GENERAL ELECTION POLITICAL PARTY MANIFESTOS** ............................................ 4

THE 2010 CONSERVATIVE PARTY MANIFESTO ........................................................................ 5

THE 2010 LIBERAL DEMOCRAT MANIFESTO ........................................................................... 16

THE 2010 LABOUR PARTY MANIFESTO .................................................................................. 30

---

**PART 2**

**THE COALITION AND CIVIL LIBERTIES** ........................................................................... 33

THE CONSERVATIVE PARTY .............................................................................................. 34

THE LIBERAL DEMOCRAT PARTY ........................................................................................ 36

---

**PART 3**

**THE 2015 GENERAL ELECTION**

**THE BIG BROTHER WATCH MANIFESTO** ......................................................................... 39

**ABOUT BIG BROTHER WATCH** ....................................................................................... 53
CONTENTS

INTRODUCTION ................................................................................................................................. 1
ABOUT THE MANIFESTO .................................................................................................................. 2

PART 1
THE 2010 GENERAL ELECTION POLITICAL PARTY MANIFESTOS ............................................... 4
THE 2010 CONSERVATIVE PARTY MANIFESTO ............................................................................. 5
THE 2010 LIBERAL DEMOCRAT MANIFESTO .................................................................................. 16
THE 2010 LABOUR PARTY MANIFESTO ......................................................................................... 30

PART 2
THE COALITION AND CIVIL LIBERTIES ......................................................................................... 33
THE CONSERVATIVE PARTY ........................................................................................................... 34
THE LIBERAL DEMOCRAT PARTY ..................................................................................................... 36

PART 3
THE 2015 GENERAL ELECTION
THE BIG BROTHER WATCH MANIFESTO ..................................................................................... 39
ABOUT BIG BROTHER WATCH ........................................................................................................ 53
INTRODUCTION

At the 2010 General Election the three main political parties made a series of manifesto commitments to strengthen the freedoms and privacy of the British public. With the creation of the Coalition Government further promises were made in the Coalition Agreement. Some of these promises were kept, but most have been watered down or entirely swept aside.

There have been some successes. ID cards were scrapped, pre-charge detention was reduced to 14 days and 1.7 million DNA profiles have been deleted. We also welcomed fairer libel laws, the removal of ‘offensive’ from Section 5 of the Public Order Act, the reform of Stop and Search and the creation of the Protection of Freedoms Act which, amongst other things, reformed the way biometric technology can be used in schools.

Yet, for every positive step we have witnessed a number of negative moves, proving that lessons from the past have not been learned. The Data Retention and Investigatory Powers Act was passed as emergency legislation with the bare minimum of debate, the extension of secret courts in the Justice and Security Act, the introduction of the Counter Terrorism and Security Bill, as well as the ongoing threat of a ‘snoopers charter’. They all emphasise that wherever they can, the Government can and will easily trade our individual liberty for collective security.

Shockingly, in these tumultuous times it has become incredibly easy for legislation to be made with only the faintest thought of how the world will look tomorrow.

As the ‘internet of things’ expands, our health, homes, travel, energy, work and play will be connected to everything everywhere. We will be required to hand over greater levels of data to ensure basic and fundamental services. Our online DNA will be as critical to the country’s economic infrastructure as to the security infrastructure.

This is despite the revelations by Edward Snowden, which opened our eyes to what governments and big business do when we aren’t as conscientious about our data as we ought to be. As the threats change and technology advances we are losing time to ensure that our online world is treated with the same protection and security as our real life world.

Big Brother Watch therefore propose ten key areas we would like to see considered in the General Election manifestos for 2015, in order to ensure the necessary balances are enacted. The proposals also consider the issue of online freedom by recommending changes to the laws governing social media and the process by which internet sites can be censored.

ABOUT THE MANIFESTO

PART 1

Looks at the pledges made before the 2010 General Election by the Conservative, Labour and Liberal Democrat parties.

PART 2

Addresses the commitments made in the Coalition Agreement by the Conservatives and the Liberal Democrats following the 2010 General Election.

PART 3

Is Big Brother Watch’s manifesto for the 2015 General Election. This section highlights the ten key areas that Big Brother Watch believe require urgent attention in order to protect and enhance our civil liberties. The topics range from ensuring that the activities of our intelligence services are properly overseen to protecting members of the public from unwanted intrusion into their homes.

THE TEN KEY AREAS OF THE BIG BROTHER WATCH MANIFESTO ARE:

1: SURVEILLANCE TRANSPARENCY
2: DATA PROTECTION
3: CCTV
4: POWERS OF ENTRY
5: COUNTER-TERRORISM STRATEGY
6: SOCIAL MEDIA LAW
7: ONLINE CENSORSHIP
8: DIGITAL BILL OF RIGHTS
9: DATA RETENTION AND INVESTIGATORY POWERS
10: INTERCEPT AS EVIDENCE

BIG BROTHER WATCH

RENATE SAMSON, CHIEF EXECUTIVE
EMMA CARR, DIRECTOR
**INTRODUCTION**

At the 2010 General Election the three main political parties made a series of manifesto commitments to strengthen the freedoms and privacy of the British public. With the creation of the Coalition Government further promises were made in the Coalition Agreement. Some of these promises were kept, but most have been watered down or entirely swept aside.

There have been some successes. ID cards were scrapped, pre-charge detention was reduced to 14 days and 1.7 million DNA profiles have been deleted. We also welcomed fairer libel laws, the removal of ‘offensive’ from Section 5 of the Public Order Act, the reform of Stop and Search and the creation of the Protection of Freedoms Act which, amongst other things, reformed the way biometric technology can be used in schools.

Yet, for every positive step we have witnessed a number of negative moves, proving that lessons from the past have not been learned. The Data Retention and Investigatory Powers Act was passed as emergency legislation with the bare minimum of debate, the extension of secret courts in the Justice and Security Act, the introduction of the Counter Terrorism and Security Bill, as well as the ongoing threat of a ‘snoopers charter’. They all emphasise that wherever they can, the Government can and will easily trade our individual liberty for collective security.

Shockingly, in these tumultuous times it has become incredibly easy for legislation to be made with only the faintest thought of how the world will look tomorrow.

As the ‘internet of things’ expands, our health, homes, travel, energy, work and play will be connected to everything everywhere. We will be required to hand over greater levels of data to ensure basic and fundamental services. Our online DNA will be as critical to the country’s economic infrastructure as to the security infrastructure.

This is despite the revelations by Edward Snowden, which opened our eyes to what governments and big business do when we aren’t as conscientious about our data as we ought to be. As the threats change and technology advances we are losing time to ensure that our online world is treated with the same protection and security as our real life world.

Big Brother Watch therefore propose ten key areas we would like to see considered in the General Election manifestos for 2015, in order to ensure the necessary balances are enacted.

THE TEN KEY AREAS OF THE BIG BROTHER WATCH MANIFESTO ARE:

1. **SURVEILLANCE TRANSPARENCY**
2. **DATA PROTECTION**
3. **CCTV**
4. **POWERS OF ENTRY**
5. **COUNTER-TERRORISM STRATEGY**
6. **SOCIAL MEDIA LAW**
7. **ONLINE CENSORSHIP**
8. **DIGITAL BILL OF RIGHTS**
9. **DATA RETENTION AND INVESTIGATORY POWERS**
10. **INTERCEPT AS EVIDENCE**

**ABOUT THE MANIFESTO**

**PART 1**

Looks at the pledges made before the 2010 General Election by the Conservative, Labour and Liberal Democrat parties.

**PART 2**

Addresses the commitments made in the Coalition Agreement by the Conservatives and the Liberal Democrats following the 2010 General Election.

**PART 3**

Is Big Brother Watch’s manifesto for the 2015 General Election. This section highlights the ten key areas that Big Brother Watch believe require urgent attention in order to protect and enhance our civil liberties. The topics range from ensuring that the activities of our intelligence services are properly overseen to protecting members of the public from unwanted intrusion into their homes.

The proposals also consider the issue of online freedom by recommending changes to the laws governing social media and the process by which internet sites can be censored.

**RENATE SAMSON, CHIEF EXECUTIVE**

**EMMA CARR, DIRECTOR**
In brief, these policy recommendations include:

1. SURVEILLANCE TRANSPARENCY
   - A review into the operation of the Commissioner system
   - A full review into necessary reform of the Intelligence and Security Committee
   - The publication of Government transparency reports

2. DATA PROTECTION
   - The introduction of custodial sentences and criminal records for the most serious Section 55 of the Data Protection Act offences
   - Extend the Data Protection Act 1998 to cover anonymised data and the ‘internet of things’

3. CCTV
   - The creation of a single point of contact to resolve CCTV complaints and grievances
   - The release of a single, enforceable Code of Practice which applies to all CCTV cameras

4. POWERS OF ENTRY
   - A new zero-based review process
   - The introduction of statutory protection
   - The creation of an enforceable Code of Practice

5. COUNTER-TERROISM STRATEGY
   - Control of the UK’s counter-terrorism strategy should be given to the National Crime Agency
   - The National Crime Agency should increase its accountability to the public

6. SOCIAL MEDIA LAW
   - A redraft of legislation to reflect changes in technology

7. ONLINE CENSORSHIP
   - A clear approach to filtering arrangements
   - The implementation of a legally sound blocking process

8. DIGITAL BILL OF RIGHTS
   - The introduction of a Digital Bill of Rights

9. DATA RETENTION AND INVESTIGATORY POWERS
   - Creation of an independent privacy and civil liberties board
   - Thorough scrutiny before the expiration of the 2016 sunset clause

10. INTERCEPT AS EVIDENCE
    - Lift the bar on the use of intercept as evidence in court
In brief, these policy recommendations include:

1. **SURVEILLANCE TRANSPARENCY**
   - A review into the operation of the Commissioner system
   - A full review into necessary reform of the Intelligence and Security Committee
   - The publication of Government transparency reports

2. **DATA PROTECTION**
   - The introduction of custodial sentences and criminal records for the most serious Section 55 of the Data Protection Act offences
   - Extend the Data Protection Act 1998 to cover anonymised data and the ‘internet of things’

3. **CCTV**
   - The creation of a single point of contact to resolve CCTV complaints and grievances
   - The release of a single, enforceable Code of Practice which applies to all CCTV cameras

4. **POWERS OF ENTRY**
   - A new zero-based review process
   - The introduction of statutory protection
   - The creation of an enforceable Code of Practice

5. **COUNTER-TERROIRISM STRATEGY**
   - Control of the UK’s counter-terrorism strategy should be given to the National Crime Agency
   - The National Crime Agency should increase its accountability to the public

6. **SOCIAL MEDIA LAW**
   - A redraft of legislation to reflect changes in technology

7. **ONLINE CENSORSHIP**
   - A clear approach to filtering arrangements
   - The implementation of a legally sound blocking process

8. **DIGITAL BILL OF RIGHTS**
   - The introduction of a Digital Bill of Rights

9. **DATA RETENTION AND INVESTIGATORY POWERS**
   - Creation of an independent privacy and civil liberties board
   - Thorough scrutiny before the expiration of the 2016 sunset clause

10. **INTERCEPT AS EVIDENCE**
    - Lift the bar on the use of intercept as evidence in court
This section provides analysis of the relevant pledges made in the Conservative Party 2010 General Election Manifesto. The areas covered are:

1. **Scrap ID Cards, the National Identity Register and the ContactPoint Database**
2. **Strengthen the Information Commissioner’s Powers**
3. **Curb Powers of Entry**
4. **Review Libel Laws**
5. **Remove the DNA of Innocent People from the National DNA Database**
6. **Reform Criminal Records Bureau Checks**
7. **Make Privacy Impact Assessments Mandatory for Data Proposals**
8. **Prevent Use of Anti-Terrorism Laws for Minor Incidents**
9. **Scrutiny of New Powers of Data-Sharing**
10. **Create a UK Bill of Rights**

**The Pledge:**
The Conservative Party pledged to return personal privacy to individuals, stating that previous approaches had been “intrusive, ineffective and enormously expensive”.

**The Outcome:**
The 2010 Identity Documents Act’s main purpose was to repeal the 2006 Identity Cards Act; abolishing identity cards and the National Identity Register.

**The Conclusion:**
ID cards would have enabled government departments and companies to share a huge amount of individuals’ personal data; allowing the state to continuously track every British citizen’s movements. ContactPoint was also unnecessary, flawed, dangerously unstable and a violation of the privacy of 11 million children.

---

2. Ibid.
4. ContactPoint: A Government database that held information on all under-18s in England. It was created in response to the death of Victoria Climbie and aimed to improve child protection by improving the way information is shared between relevant services. It was criticised on privacy, security and child safety grounds.
This section provides analysis of the relevant pledges made in the Conservative Party 2010 General Election Manifesto. The areas covered are:

1. Scrap ID cards, the National Identity Register and the ContactPoint database
2. Strengthen the Information Commissioner’s Powers
3. Curb powers of entry
4. Review Libel Laws
5. Remove the DNA of innocent people from the National DNA database
6. Reform Criminal Records Bureau checks
7. Make privacy impact assessments mandatory for data proposals
8. Prevent use of anti-terrorism laws for minor incidents
9. Scrutiny of new powers of data-sharing
10. Create a UK Bill of Rights

THE 2010 CONSERVATIVE PARTY MANIFESTO

THE PLEDGE:
The Conservative Party pledged to return personal privacy to individuals, stating that previous approaches had been “intrusive, ineffective and enormously expensive”. As a result the Manifesto included plans to “scrap ID cards, the National Identity Register and the ContactPoint database”.

THE OUTCOME:
The 2010 Identity Documents Act’s main purpose was to repeal the 2006 Identity Cards Act; abolishing identity cards and the National Identity Register. Damian Green MP, Minister for Policing, Criminal Justice and Victims, stated:

“Laying ID cards to rest demonstrates the government’s commitment to scale back the power of the state and restore civil liberties. It is about the people having trust in the government to know when it is necessary and appropriate for the state to hold and use personal data.”

Also, on 22 July 2010, the Children and Families Minister, Tim Loughton MP, confirmed that ContactPoint would be shut down on 6 August 2010. He stated that:

“I wasn’t wrong to switch off this flawed child register. ContactPoint failed to protect our children – it prioritised data input over social work.”

THE CONCLUSION:
ID cards would have enabled government departments and companies to share a huge amount of individuals’ personal data; allowing the state to continuously track every British citizen’s movements. ContactPoint was also unnecessary, flawed, dangerously unstable and a violation of the privacy of 11 million children.

Big Brother Watch welcomed the abolition of ID cards, the National Identity Registration and the ContactPoint Database.

[Refs]
3. ContactPoint: A Government database that held information on all under 18s in England. It was created in response to the death of Victoria Climbie and aimed to improve child protection by improving the way information is shared between relevant services. It was criticised on privacy, security and child safety grounds.
THE PLEDGE:
The Conservative Party pledged to give individuals more control over their data, stating “we believe that personal data should be controlled by individual citizens themselves”. The Manifesto declared that a Conservative Government would: “strengthen the powers of the Information Commissioner to penalise any public body found guilty of mismanaging data”.\(^\text{7, 8}\)

THE OUTCOME:
On 26 May 2011, the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 (PECR) came into force, enhancing the enforcement powers of the Information Commissioner laid out in the 2003 Regulations.\(^\text{9, 10}\)
The PECR enables the ICO to:

• Impose civil monetary penalties of up to £500,000 for serious breaches of Privacy and Electronic Communications Regulations (PECR)
• Impose a fixed monetary penalty of £1,000 on a service provider that does not comply with the new breach notification requirements
• Require a communications provider to give the Commissioner the information needed to investigate the compliance of any person with PECR
• Inspect the measures taken by a provider of public electronic communications services to safeguard the security of that service and to comply with the new personal data breach notification and recording requirements

However, this amendment was made by the European Union and not by the Coalition Government.

THE CONCLUSION:
Whilst the powers of the Information Commissioner have been strengthened, the penalties still do not appropriately reflect the serious implications of breaching the Data Protection Act 1998. The amendments to the Privacy and Electronic Communications Regulations were not enough to prevent recurring breaches or to eliminate lax attitudes to data protection.

In light of the continued increase in the use of big data and the proliferation of data sharing programmes, it is Big Brother Watch’s belief that further work should be carried out on the effectiveness of the Data Protection Act to ensure that there is an effective deterrent to prevent individuals from deliberately taking others’ personal information.

---

8. Ibid.\(^\text{a}\)

---

2. STRENGTHEN THE INFORMATION COMMISSIONER’S POWERS

3. CURB POWERS OF ENTRY

THE PLEDGE:
The Conservative Party pledged to “take further steps to protect people from unwarranted intrusion by the state, including cutting back intrusive powers of entry into homes”.\(^\text{11}\)

THE OUTCOME:
The Protection of Freedoms Act, received royal assent and became law on 1st May 2012. It required Secretaries of State to review the powers of entry their departments are responsible for. The process was scheduled to take place over two years, between the Bill gaining Royal Assent and mid-2014. Progress reports would be published every six months to update both Parliament and members of the public on how process was moving forward. The purpose of the scheme was to ensure that all powers were still necessary, proportionate and contained sufficient safeguards.

THE CONCLUSION:
The Protection of Freedoms Act set a two year deadline of May 2014 for formal ministerial responses. In December 2014 a majority of the relevant departments had published their final reports.

In a written statement James Brokenshire, Minister for Security and Immigration, confirmed that the number of powers would be reduced, from 1237 to 912, a fall of 325, additionally further safeguards will be added to 231 powers.\(^\text{12}\) Whilst this is a welcome reduction the issue of the number of officials who can use the powers still remains. It should be the case that only those who need the powers to carry out their roles should have them. It is also disappointing that the review failed to use a ‘zero-based’ approach, which would have allowed departments to identify only those powers that were necessary.

A further concern is that whilst a Code of Practice for powers of entry has now been produced it contains no sanctions for those who breach its terms. Additionally throughout there is a lack of clarity emphasised by the repeated use of the word ‘reasonable’.

---

2. STRENGTHEN THE INFORMATION COMMISSIONER’S POWERS

THE PLEDGE:
The Conservative Party pledged to give individuals more control over their data, stating “we believe that personal data should be controlled by individual citizens themselves”. The Manifesto declared that a Conservative Government would: “strengthen the powers of the Information Commissioner to penalise any public body found guilty of mismanaging data”. 7,8

THE OUTCOME:
On 26 May 2011, the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 (PECR) came into force, enhancing the enforcement powers of the Information Commissioner laid out in the 2003 Regulations. 9,10

The PECR enables the ICO to:
- Impose civil monetary penalties of up to £500,000 for serious breaches of Privacy and Electronic Communications Regulations (PECR)
- Impose a fixed monetary penalty of £1,000 on a service provider that does not comply with the new breach notification requirements
- Require a communications provider to give the Commissioner the information needed to investigate the compliance of any person with PECR
- Inspect the measures taken by a provider of public electronic communications services to safeguard the security of that service and to comply with the new personal data breach notification and recording requirements

However, this amendment was made by the European Union and not by the Coalition Government.

THE CONCLUSION:
Whilst the powers of the Information Commissioner have been strengthened, the penalties still do not appropriately reflect the serious implications of breaching the Data Protection Act 1998. The amendments to the Privacy and Electronic Communications Regulations were not enough to prevent recurring breaches or to eliminate lax attitudes to data protection.

In light of the continued increase in the use of big data and the proliferation of data sharing programmes, it is Big Brother Watch’s belief that further work should be carried out on the effectiveness of the Data Protection Act to ensure that there is an effective deterrent to prevent individuals from deliberately taking others’ personal information.

3. CURB POWERS OF ENTRY

THE PLEDGE:
The Conservative Party pledged to “take further steps to protect people from unwarranted intrusion by the state, including cutting back intrusive powers of entry into homes”. 11

THE OUTCOME:
The Protection of Freedoms Act, received royal assent and became law on 1st May 2012. It required Secretaries of State to review the powers of entry their departments are responsible for. The process was scheduled to take place over two years, between the Bill gaining Royal Assent and mid-2014. Progress reports would be published every six months to update both Parliament and members of the public on how process was moving forward. The purpose of the scheme was to ensure that all powers were still necessary, proportionate and contained sufficient safeguards.

THE CONCLUSION:
The Protection of Freedoms Act set a two year deadline of May 2014 for formal ministerial responses. In December 2014 a majority of the relevant departments had published their final reports.

In a written statement James Brokenshire, Minister for Security and Immigration, confirmed that the number of powers would be reduced, from 1237 to 912, a fall of 325, additionally further safeguards will be added to 231 powers. 12 Whilst this is a welcome reduction the issue of the number of officials who can use the powers still remains. It should be the case that only those who need the powers to carry out their roles should have them. It is also disappointing that the review failed to use a ‘zero-based’ approach, which would have allowed departments to identify only those powers that were necessary.

A further concern is that whilst a Code of Practice for powers of entry has now been produced it contains no sanctions for those who breach its terms. Additionally throughout there is a lack of clarity emphasised by the repeated use of the word ‘reasonable’.

8. Ibid.
4. REVIEW LIBEL LAWS

THE PLEDGE:
The Conservative Party pledged that in order to “protect freedom of speech, reduce costs and discourage libel tourism,” they will “review and reform libel laws”. 13

THE OUTCOME:
The Defamation Act came into force on 1 January 2014, containing a series of measures to protect freedom of speech. They included the following:
- Claimants must be able to show that they have suffered serious harm before they can sue for defamation
- A defence for those publishing material on a matter that is in the public interest
- The increase in protection to operators of websites that host user-generated content provided they comply with the procedure to enable the complainant to resolve disputes directly with the author of the material concerned
- Defence of truth and honest opinion to replace the common law defences of justification and fair comment
- Tightening the test for claims involving those with little connection to England and Wales being brought before the courts to target libel tourism
- Single-publication rule to prevent repeated claims against a publisher about the same material

THE CONCLUSION:
We welcome the Defamation Act 2014 and the positive impact it has had on freedom of expression in England and Wales, however the new measures contained within the Defamation Act have not been able to extend to Northern Ireland, leaving the citizens of Northern Ireland with few and restricted rights to free speech.

The Libel Reform Campaign has stated that this has:
“Created a loophole in the law. Libel lawyers have already begun touting Belfast to potential litigants as a claimant friendly jurisdiction. This creates uncertainty and confusion for journalists and publishers throughout the United Kingdom”. 15


5. REMOVE THE DNA OF INNOCENT PEOPLE FROM THE NATIONAL DNA DATABASE

THE PLEDGE:
The Conservative Party stated that: “The indefinite retention of innocent people’s DNA is unacceptable…Will legislate to make sure that our DNA database is used primarily to store information about those who are guilty of committing crimes rather than those who are innocent”. 16

THE OUTCOME:
The Protection of Freedoms Act 2012 included measures to remove the DNA records of more than one million innocent adults and children. The Act enables DNA samples of convicted individuals to stay on the database for three years. This can be extended by court order for a further three years.

In 2013, Criminal Information Minister Lord Taylor of Holbeach said:
“Over 1.7 million DNA profiles taken from innocent people and from children have been removed from the DNA database. The destruction of all 7,753,000 DNA samples is a significant step to protect the genetic privacy of people in the United Kingdom.”

THE CONCLUSION:
Although the deletion of more than 1.7 million DNA profiles taken from innocent people and children is a good first step, there are still some issues that the Protection of Freedoms Act did not address. These include:
- Indefinite retention of DNA profiles from adults who have committed a minor offence and children who have committed more than one minor offence, is still disproportionate
- Collection of DNA on arrest for all recordable offences even if DNA is not relevant to solving the crime is unnecessary and expensive
- The length of time that the Police National Computer records are retained for innocent people and those who committed minor offences is still unclear

Therefore, more can still be done to ensure that only the most necessary samples are kept on the National DNA database.

Big Brother Watch maintain that the wholesale implementation of the ‘Scottish Model’ for DNA retention would be preferable to the existing arrangements. Whilst the Coalition have made some changes it is important that they continue to reform retention policies to bring them in line with the fairer and less permissive system in Scotland.

4. REVIEW LIBEL LAWS

THE PLEDGE:
The Conservative Party pledged that in order to “protect freedom of speech, reduce costs and discourage libel tourism,” they will “review and reform libel laws.”

THE OUTCOME:
The Defamation Act came into force on 1 January 2014, containing a series of measures to protect freedom of speech. They included the following:

• Claimants must be able to show that they have suffered serious harm before they can sue for defamation
• A defence for those publishing material on a matter that is in the public interest
• The increase in protection to operators of websites that host user-generated content provided they comply with the procedure to enable the complainant to resolve disputes directly with the author of the material concerned
• Defence of truth and honest opinion to replace the common law defences of justification and fair comment
• Tightening the test for claims involving those with little connection to England and Wales being brought before the courts to target libel tourism
• Single-publication rule to prevent repeated claims against a publisher about the same material

THE CONCLUSION:
We welcome the Defamation Act 2014 and the positive impact it has had on freedom of expression in England and Wales, however the new measures contained within the Defamation Act have not been able to extend to Northern Ireland, leaving the citizens of Northern Ireland with few and restricted rights to free speech. 

The Libel Reform Campaign has stated that this has:
“Created a loophole in the law. Libel lawyers have already begun touting Belfast to potential litigants as a claimant friendly jurisdiction. This creates uncertainty and confusion for journalists and publishers throughout the United Kingdom.”

5. REMOVE THE DNA OF INNOCENT PEOPLE FROM THE NATIONAL DNA DATABASE

THE PLEDGE:
The Conservative Party stated that: “The indefinite retention of innocent people’s DNA is unacceptable…Will legislate to make sure that our DNA database is used primarily to store information about those who are guilty of committing crimes rather than those who are innocent.”

THE OUTCOME:
The Protection of Freedoms Act 2012 included measures to remove the DNA records of more than one million innocent adults and children. The Act enables DNA samples of convicted individuals to stay on the database for three years. This can be extended by court order for a further three years.

In 2013, Criminal Information Minister Lord Taylor of Holbeach said: “Over 1.7 million DNA profiles taken from innocent people and from children have been removed from the DNA database. The destruction of all 7,753,000 DNA samples is a significant step to protect the genetic privacy of people in the United Kingdom.”

THE CONCLUSION:
Although the deletion of more than 1.7 million DNA profiles taken from innocent people and children is a good first step, there are still some issues that the Protection of Freedoms Act did not address. These include:

• Indefinite retention of DNA profiles from adults who have committed a minor offence and children who have committed more than one minor offence, is still disproportionate
• Collection of DNA on arrest for all recordable offences even if DNA is not relevant to solving the crime is unnecessary and expensive
• The length of time that the Police National Computer records are retained for innocent people and those who committed minor offences is still unclear

Therefore, more can still be done to ensure that only the most necessary samples are kept on the National DNA database.

Big Brother Watch maintain that the wholesale implementation of the ‘Scottish Model’ for DNA retention would be preferable to the existing arrangements. Whilst the Coalition have made some changes it is important that they continue to reform retention policies to bring them in line with the fairer and less permissive system in Scotland.
6. REFORM CRIMINAL RECORDS BUREAU CHECKS

THE PLEDGE:
The Conservative Party stated that “people working in positions of trust with children should go through a proper criminal record check”. However, they argued that the previous CRB checks went too far. Therefore, the Conservatives pledged that they would “review the criminal records and ‘vetting and barring’ regime and scale it back to common sense levels”.

THE OUTCOME:
In January 2013, the Court of Appeal ruled that CRB checks were ‘incompatible with Human Rights Act.’ In May 2013 the Home Office announced changes to the CRB system, creating the Disclosure and Barring Service (DBS).
The new system brought with it a number of changes, including the following:
• A new definition of ‘regulated activity’ or the work that someone who has been barred by the Independent Safeguarding Authority must not do
• A repeal of the controlled activity category, which covered people who might have more infrequent contact with vulnerable groups
• The repeal of registration and continuous monitoring, in the original plans the scheme would have required people to register to work with vulnerable groups and would have allowed them to be continuously monitored for new criminal record information
• A repeal of additional information, this power, which existed under the Police Act 1997 allowed forces to disclose additional information to organisations
• The minimum age at which someone can apply for a CRB check was changed to 16, before this there was no age restriction
• A more rigorous ‘relevancy’ test for when the police release information held locally on an enhanced CRB check

THE CONCLUSION:
The reforms to CRB checks, and the impact this has had on individuals’ ability to get jobs, is welcomed. The new DBS system has seen a much more common sense approach to a system that was ruining people’s lives. It strikes a clear balance between protecting children and vulnerable groups and preventing intrusion into people’s personal lives.
This is not to say that the reforms have been completely successful. In many cases there has been a lack of clear explanation about how the system has been changed. This has left people unsure of what their responsibilities are. Even more worrying is that many people are unaware of how to get an incorrect entry removed. This can have a major impact on their ability to gain employment.

7. MAKE PRIVACY IMPACT ASSESSMENTS MANDATORY FOR DATA PROPOSALS

THE PLEDGE:
The Conservative Party pledged that they would make “Privacy Impact Assessments of any proposal that involves data collection or sharing” compulsory.

THE OUTCOME:
The European Commission introduced its proposed Data Protection Regulation in January 2012. Article 33 of this regulation makes Data Protection Impact Assessments (DPIAs) mandatory for public and private sector organisations throughout Europe. However, there is a difference between DPIAs and Privacy Impact Assessments (PIAs).
According to the PIA Handbook, a PIA should not only consider personal data but also four different types of privacy:
• Privacy of personal information
• Privacy of the person
• Privacy of personal behaviour
• Privacy of personal communication
Additionally, it is important to note that it was the European Commission that made DPIAs mandatory. Despite their pledge, the Conservative Party has not made any form of privacy or data protection impact assessment compulsory.

THE CONCLUSION:
Research carried out by Trilateral Research & Consulting highlights that “more than two-thirds of responding organisations have done a PIA”. However, the research was only able to survey a tiny fraction of companies as the organisation noted that “it was extremely difficult to compile contacts for private companies”. Despite this, the report highlights that the Conservative Party has not followed through on their pledge to make PIAs compulsory. Although DPIAs are required, they fall short of ensuring maximum protection for individuals’ privacy. More needs to be done to ensure that PIAs are mandatory for all cases involving individuals’ private information.

6. Reform Criminal Records Bureau Checks

The Conservative Party pledged that they would make “Privacy Impact Assessments of any proposal that involves data collection or sharing” compulsory.23

The Pledge:

The Conservative Party stated that “people working in positions of trust with children should go through a proper criminal record check”.20 However, they argued that the previous CRB checks went too far. Therefore, the Conservatives pledged that they would “review the criminal records and ‘vetting and barring’ regime and scale it back to common sense levels”.21

The Outcome:

In January 2013, the Court of Appeal ruled that CRB checks were ‘incompatible with Human Rights Act.’22 In May 2013 the Home Office announced changes to the CRB system, creating the Disclosure and Barring Service (DBS).

The new system brought with it a number of changes, including the following:

- A new definition of ‘regulated activity’ or the work that someone who has been barred by the Independent Safeguarding Authority must not do
- A repeal of the controlled activity category, which covered people who might have more infrequent contact with vulnerable groups
- The repeal of registration and continuous monitoring, in the original plans the scheme would have required people to register to work with vulnerable groups and would have allowed them to be continuously monitored for new criminal record information
- A repeal of additional information, this power, which existed under the Police Act 1997 allowed forces to disclose additional information to organisations
- The minimum age at which someone can apply for a CRB check was changed to 16, before this there was no age restriction
- A more rigorous ‘relevancy’ test for when the police release information held locally on an enhanced CRB check

The Conclusion:

The reforms to CRB checks, and the impact this has had on individuals’ ability to get jobs, is welcomed. The new DBS system has seen a much more common sense approach to a system that was ruining people’s lives. It strikes a clear balance between protecting children and vulnerable groups and preventing intrusion into people’s personal lives.

This is not to say that the reforms have been completely successful. In many cases there has been a lack of clear explanation about how the system has been changed. This has left people unsure of what their responsibilities are. Even more worrying is that many people are unaware of how to get an incorrect entry removed. This can have a major impact on their ability to gain employment.

7. Make Privacy Impact Assessments Mandatory for Data Proposals

The Pledge:

The European Commission introduced its proposed Data Protection Regulation in January 2012. Article 33 of this regulation makes Data Protection Impact Assessments (DPIAs) mandatory for public and private sector organisations throughout Europe.26 25

However, there is a difference between DPIAs and Privacy Impact Assessments (PIAs). According to the PIA Handbook, a PIA should not only consider personal data but also four different types of privacy:

- Privacy of personal information
- Privacy of the person
- Privacy of personal behaviour
- Privacy of personal communication

Additionally, it is important to note that it was the European Commission that made DPIAs mandatory. Despite their pledge, the Conservative Party has not made any form of privacy or data protection impact assessment compulsory.

The Conclusion:

Research carried out by Trilateral Research & Consulting highlights that “more than two-thirds of responding organisations have done a PIA”.27 28 However, the research was only able to survey a tiny fraction of companies as the organisation noted that “it was extremely difficult to compile contacts for private companies”29 Despite this, the report highlights that the Conservative Party has not followed through on their pledge to make PIAs compulsory.

Although DPIAs are required, they fall short of ensuring maximum protection for individuals’ privacy. More needs to be done to ensure that PIAs are mandatory for all cases involving individuals’ private information.

---

24. Ibid.
28. Ibid.
29. Ibid.

8. PREVENT USE OF ANTI-TERRORISM LAWS FOR MINOR INCIDENTS

THE PLEDGE:
The Conservative Party pledged that they would amend the Regulation of Investigatory Powers Act 2000 (RIPA) to curtail “surveillance powers that allow some councils to use anti-terrorism laws to spy on people making trivial mistakes or minor breaches of the rules”.

THE OUTCOME:
On 26 January 2011, the Home Office published a Review of Counter-Terrorism and Security Powers, exploring local authorities’ use of surveillance to investigate minor offences. The review recommended that surveillance carried out under RIPA should firstly be authorised by a magistrate and should only be used to investigate offences that carry a custodial sentence of over 6 months.

The Protection of Freedoms Act 2012 states that all local authority surveillance authorised under the RIPA will have to be approved by a magistrate. It should, however, be noted that no such warrants are required for investigations carried out by the police or other public authorities.

The Office of Surveillance Commissioners 2013-14 annual report was critical of the lack of knowledge, understanding and training displayed by magistrates regarding RIPA. The report also highlighted the Commissioner’s concerns that officials in public authorities may be wilfully ignoring RIPA by covertly using social media to carry out investigations.

THE CONCLUSION:
Although Big Brother Watch welcomes the requirement of judicial authorisation for local authorities, there are still many fundamental issues with the disproportionate use of RIPA which need to be addressed. These issues include:

• The lack of transparency around the use of the powers. Although local authorities must seek the approval of the magistrate, the public are still unaware about what surveillance is taking place, how often, for what purpose, or what the outcome is. This data should be made available to the public.

• Anti-terrorism legislation continues to be misused. Judicial authorisation should be a requirement for all authorities wishing to use RIPA and not just for local authorities.

• The legislation is out of date. The newly announced review into communications data and interception powers must now be seen as an opportunity to properly update RIPA.

9. SCRUTINY OF NEW POWERS OF DATA-SHARING

THE PLEDGE:
The Conservative Party pledged to ensure “proper Parliamentary scrutiny of any new powers of data-sharing”.

THE OUTCOME:
This pledge did not feature in the Coalition Agreement. Subsequently, the Coalition Government did not attempt to increase proper Parliamentary scrutiny of new powers of data-sharing.

THE CONCLUSION:
The current level of scrutiny is wholly unsatisfactory. Data sharing schemes, such as care.data, are being rushed through with little thought given to their implications. The scrutiny of major data sharing proposals is not what it could be. A good example of this is the care.data scheme. Although there was scrutiny by the Health Select Committee it came far too late. The Committee held its first oral evidence session on the proposed database on the 24th February 2014. This was after the Government had announced that the scheme was to be delayed. Pre-legislative scrutiny should be arranged for any future data sharing schemes to ensure that proper consideration and oversight can be made by parliamentarians and the public alike.

31. Ibid p.21
8. PREVENT USE OF ANTI-TERRORISM LAWS FOR MINOR INCIDENTS

THE PLEDGE:
The Conservative Party pledged that they would amend the Regulation of Investigatory Powers Act 2000 (RIPA) to curtail “surveillance powers that allow some councils to use anti-terrorism laws to spy on people making trivial mistakes or minor breaches of the rules”.

THE OUTCOME:
On 26 January 2011, the Home Office published a Review of Counter-Terrorism and Security Powers, exploring local authorities’ use of surveillance to investigate minor offences. The review recommended that surveillance carried out under RIPA should firstly be authorised by a magistrate and should only be used to investigate offences that carry a custodial sentence of over 6 months.

The Protection of Freedoms Act 2012 states that all local authority surveillance authorised under the RIPA will have to be approved by a magistrate. It should, however, be noted that no such warrants are required for investigations carried out by the police or other public authorities.

The Office of Surveillance Commissioners 2013-14 annual report was critical of the lack of knowledge, understanding and training displayed by magistrates regarding RIPA. The report also highlighted the Commissioner’s concerns that officials in public authorities may be wilfully ignoring RIPA by covertly using social media to carry out investigations.

THE CONCLUSION:
Although Big Brother Watch welcomes the requirement of judicial authorisation for local authorities, there are still many fundamental issues with the disproportionate use of RIPA which need to be addressed. These issues include:

- **The lack of transparency around the use of the powers.** Although local authorities must seek the approval of the magistrate, the public are still unaware about what surveillance is taking place, how often, for what purpose, or what the outcome is. This data should be made available to the public.

- **Anti-terrorism legislation continues to be misused.** Judicial authorisation should be a requirement for all authorities wishing to use RIPA and not just for local authorities.

- **The legislation is out of date.** The newly announced review into communications data and interception powers must now be seen as an opportunity to properly update RIPA.

9. SCRUTINY OF NEW POWERS OF DATA-SHARING

THE PLEDGE:
The Conservative Party pledged to ensure “proper Parliamentary scrutiny of any new powers of data-sharing”.

THE OUTCOME:
This pledge did not feature in the Coalition Agreement. Subsequently, the Coalition Government did not attempt to increase proper Parliamentary scrutiny of new powers of data-sharing.

THE CONCLUSION:
The current level of scrutiny is wholly unsatisfactory. Data sharing schemes, such as care.data, are being rushed through with little thought given to their implications. The scrutiny of major data sharing proposals is not what it could be. A good example of this is the care.data scheme. Although there was scrutiny by the Health Select Committee it came far too late. The Committee held its first oral evidence session on the proposed database on the 24th February 2014. This was after the Government had announced that the scheme was to be delayed. Pre-legislative scrutiny should be arranged for any future data sharing schemes to ensure that proper consideration and oversight can be made by parliamentarians and the public alike.

---

31. Ibid p.21
The Conservative Party pledged that they would “replace the Human Rights Act with a UK Bill of Rights”.16

The Commission published its report A UK Bill of Rights? The Choice Before Us in December 2012, however members were unable to agree on a common position and the Government has not officially responded to the report yet.17

At the 2013 Conservative Party Conference, the Home Secretary, Theresa May MP, stated: “the next Conservative manifesto will promise to scrap the Human Rights Act... the Conservative position is clear – if leaving the European Convention is what it takes to fix our human rights law, that is what we should do.”18

Robert Halfon MP has tabled an Early Day Motion which states:

“This House is deeply concerned that privacy is gradually being eroded by private companies using the internet to obtain personal data and selling it for commercial gain [and]...believes an internet bill of rights is needed to guard against the growing infringement of civil liberties that are not covered by existing legislation.”19

Outside of politics, an open letter calling for an ‘international bill of digital rights’ was signed by more than 500 authors, including Ian McEwan and Sir Tom Stoppard.20 One of the strongest advocates of such a Bill has been Sir Tim Berners-Lee, who sees an “open, neutral internet” as integral to the protection of “open government, good democracy, good healthcare, connected communities and diversity of culture”.21


THE 2010 LIBERAL DEMOCRAT MANIFESTO

This section provides analysis of the relevant pledges made in the Liberal Democrat 2010 General Election Manifesto. The areas covered are:

1. Restrict Surveillance Powers of Local Authorities
2. Rebalance the US/UK Extradition Treaty
3. Defend Trial by Jury
4. Prevent the Collection of Children’s Biometric Data Without Permission
5. Restore the Right to Protest
6. Reform Libel Laws
7. Abolish ID Cards and Increase the Number of Police Officers
8. Scrap Plan for Second Generation ePassports
9. Prevent an Increase in New Offences
10. Prevent Storage of Email and Internet Records
11. Remove Innocent People’s DNA from Police Database
12. Scrap the ContactPoint Database
13. Scrap Control Orders
14. Reduce Maximum Period of Pre-Charge Detention to 14-Day Detention
THE PLEDGE:
The Conservative Party pledged that they would “replace the Human Rights Act with a UK Bill of Rights”.  

THE OUTCOME:
In March 2011, the Commission on a Bill of Rights was established “to investigate the creation of a UK Bill of Rights that incorporates and builds on all our obligations under the European Convention on Human Rights ensures that these rights continue to be enshrined in UK law, and protects and extends our liberties”.  

The Commission published its report A UK Bill of Rights? The Choice Before Us in December 2012, however members were unable to agree on a common position and the Government has not officially responded to the report yet.  

At the 2013 Conservative Party Conference, the Home Secretary, Theresa May MP, stated: “the next Conservative manifesto will promise to scrap the Human Rights Act, the Conservative position is clear – if leaving the European Convention is what it takes to fix our human rights law, that is what we should do.”  

THE CONCLUSION:
It is unclear what impact replacing the Human Rights Act with a UK Bill of Rights would have. Arguably the more important issue in this area is the mooted Digital Bill of Rights, this is something that deserves attention and would deliver real protections to our online freedoms.  

Robert Halfon MP has tabled an Early Day Motion which states: “This House is deeply concerned that privacy is gradually being eroded by private companies using the Internet to obtain personal data and selling it for commercial gain [and]...believes an internet bill of rights is needed to guard against the growing infringement of civil liberties that are not covered by existing legislation.”  

Outside of politics, an open letter calling for an ‘international bill of digital rights’ was signed by more than 500 authors, including Ian McEwan and Sir Tom Stoppard. One of the strongest advocates of such a Bill has been Sir Tim Berners-Lee, who sees an “open, neutral internet” as integral to the protection of “open government, good democracy, good healthcare, connected communities and diversity of culture”. 

THE 2010 LIBERAL DEMOCRAT MANIFESTO
This section provides analysis of the relevant pledges made in the Liberal Democrat 2010 General Election Manifesto. The areas covered are:

1. RESTRICT SURVEILLANCE POWERS OF LOCAL AUTHORITIES
2. REBALANCE THE US/UK EXTRADITION TREATY
3. DEFEND TRIAL BY JURY
4. PREVENT THE COLLECTION OF CHILDREN’S BIOMETRIC DATA WITHOUT PERMISSION
5. RESTORE THE RIGHT TO PROTEST
6. REFORM LIBEL LAWS
7. ABOLISH ID CARDS AND INCREASE THE NUMBER OF POLICE OFFICERS
8. SCRAP PLAN FOR SECOND GENERATION ePASSPORTS
9. PREVENT AN INCREASE IN NEW OFFENCES
10. PREVENT STORAGE OF EMAIL AND INTERNET RECORDS
11. REMOVE INNOCENT PEOPLE’S DNA FROM POLICE DATABASE
12. SCRAP THE CONTACTPOINT DATABASE
13. SCRAP CONTROL ORDERS
14. REDUCE MAXIMUM PERIOD OF PRE-CHARGE DETENTION TO 14-DAY DETENTION
**1. RESTRICT SURVEILLANCE POWERS OF LOCAL AUTHORITIES**

**THE PLEDGE:**

The Liberal Democrat Party pledged to “stop councils from spying on people”.\(^6\) This is in the context of Local Authorities using the Regulation of Investigatory Powers Act 2000 (RIPA) to use surveillance on local citizens and investigate minor offences.

**THE OUTCOME:**

On 26 January 2011, the Home Office published a Review of Counter-Terrorism and Security Powers, highlighting local authorities’ use of surveillance to investigate minor offences. The Protection of Freedoms Act 2012 states that all local authority surveillance authorised under the RIPA will have to be approved by a Magistrate. The amendments to RIPA mean that local authorities are no longer able to use any of the three covert investigatory techniques available to them without the approval of the magistrate. The surveillance techniques are as follows:

- Directed surveillance
- The deployment of a Covert Human Intelligence Source (CHIS)
- Accessing communications data

It should however be noted that no such warrants are required for investigations carried out by the police or other public authorities. The Office of Surveillance Commissioners 2013-14 annual report was critical of the lack of knowledge, understanding and training displayed by magistrates regarding RIPA. The report also highlighted the Commissioner’s concerns that officials in public authorities may be wilfully ignoring RIPA by covertly using social media to carry out investigations.\(^43\,44\)

**THE CONCLUSION:**

Although Big Brother Watch welcomes the requirement of judicial authorisation for local authorities, there are still many fundamental issues with RIPA and its disproportionate use that need to be addressed. These issues include:

- The continued lack of transparency. Although local authorities need to seek the approval of the magistrate, the public still do not know what the surveillance is taking place, how often, for what purpose, or what the outcome is. This data should be made available to the public
- Anti-terrorism legislation continues to be misused.\(^46\,47\) Judicial authorisation should be a requirement for all authorities wishing to use RIPA and not just for Local Authorities
- The legislation is out of date. The number of issues with RIPA itself and how it functions need to be addressed. These issues include:

  1. Legislation reiterating an outdated legal framework
  2. No centralised repository of surveillance
  3. The lack of knowledge, understanding and training displayed by magistrates regarding RIPA.


\(\text{\textsuperscript{47}}\) Ibid p.21

\(\text{\textsuperscript{48}}\) The Times, 9th September 2014, “Big Brother Watch welcomes order requiring Local Authorities to seek Magistrate’s approval for surveillance”.

\(\text{\textsuperscript{49}}\) David Miranda case: “Stop unfair extradition to the US”, Big Brother Watch looks forward to the Committee’s findings, which are expected to be published by March 2015.

\(\text{\textsuperscript{50}}\) Independent, Anger at extradition treaty review, 18th October 2011: http://www.independent.co.uk/news/uk/home-news/anger-at-extradition-treaty-review-2372276.html

\(\text{\textsuperscript{51}}\) Law Society Gazette, The Baker report on extradition law is something to build on: http://www.lawgazette.co.uk/article/3049940480

\(\text{\textsuperscript{52}}\) The JCHR, for example, considered the Transatlantic arrangement to be ‘lopsided’ and something “which allows the US to request the extradition of UK citizens without the requirement to produce evidence of an offence”.\(^49\)

**2. REBALANCE THE US/UK EXTRADITION TREATY**

**THE PLEDGE:**

In 2009, Nick Clegg MP was vocally opposed to what he saw as Gary McKinnon being “hung out to dry by a British Government desperate to appease its American counterparts”.\(^48\) As a result the Liberal Democrats pledged to “stop unfair extradition to the US”.\(^49\)

**THE OUTCOME:**

In October 2011 the Independent Review of the United Kingdom’s Extradition Arrangements led by Sir Scott Baker, a former Court of Appeal judge was established. The process involved a review of the controversial Extradition Act 2003 as well as the measures in place between the US and the UK.

Previously, committees including the Home Affairs Select Committee and the Joint Committee on Human Rights (JCHR) have criticised the US-UK Treaty.\(^46\) The JCHR, for example, considered the Transatlantic arrangement to be ‘lopsided’ and something “which allows the US to request the extradition of UK citizens without the requirement to produce evidence of an offence”.\(^49\)

In spite of the widespread expectation that the review would find the treaty to be unequal Sir Scott Baker concluded that “the United States/United Kingdom Treaty does not operate in an unbalanced manner”.\(^51\)

In June 2014 Lord Hill of Oareford announced the creation of The Committee on Extradition Law.\(^51\) Big Brother Watch looks forward to the Committee’s findings, which are expected to be published by March 2015.

**THE CONCLUSION:**

The findings of the Baker Review were attacked by a variety of figures. David Davis MP called the report ‘inexplicable’, as “the idea that the UK/US extradition treaty is in any sense symmetrical is in defiance of the facts”.\(^52\) Keith Vaz MP, chairman of the Home Affairs Select Committee, added that he was “concerned that the extradition review has not shed any light on the ease of extradition”.\(^52\) A consultant at Cubism Law, Dan Hyde, warned that the findings would “likely bring calls for the review to be reviewed”.\(^52\)
3. DEFEND TRIAL BY JURY

THE PLEDGE:
After their opposition to proposals that would have abolished trial by jury in complex fraud cases, something Simon Hughes MP warned could lead to a ‘two-tier justice system’ 57 the Liberal Democrat Party pledged to ‘defend trial by jury.’ 58

THE OUTCOME:
The Coalition Agreement did not include the defence of trial by jury. Subsequently little has been done to secure the presence of the jury in trials. Although most trials do include a jury, the issue is still contested. This can be seen in the use of secret trials as extended through the Justice and Security Act 2013.

THE CONCLUSION:
As has been warned, criminal cases being heard in secret and without a jury “risks ripping up the very tradition of open justice in the UK.” 59 The consensus is that juries are still an integral part of the British legal system, what JUSTICE call a ‘key constitutional safeguard.’ 60 The former Attorney General, Dominic Grieve MP has also stated that trial by jury is an “essential element of the justice system of England and Wales. It is deeply ingrained in our national DNA.” 61

Big Brother Watch strongly believe in the right to a trial by jury and as the 800th anniversary of Magna Carta approaches, would like to see further action taken to protect this fundamental right.

---

4. PREVENT THE COLLECTION OF CHILDREN’S BIOMETRIC DATA WITHOUT PERMISSION

THE PLEDGE:
In reaction to the increase in schools using student’s biometric data without their parents’ permission, the Liberal Democrat Party pledged to “stop children being fingerprinted at school without their parents’ permission.” 62

THE OUTCOME:
The Protection of Freedoms Act 2012 requires schools and further education institutions to:
- Obtain the written consent of parents (or others with main parental responsibility) before processing biometric information from children under the age of 18 years
- Ensure that such information is not processed if a child objects, even where a parent has consented
- Provide reasonable alternative arrangements for pupils who refuse or whose parents do not consent to biometric information being processed

THE CONCLUSION:
The move was welcomed by the Association of School and College Leavers, with the General Secretary Brian Lightman stating that “It’s right that parents give their consent to use biometric data, just as they do for taking photographs.” 63

Whilst this is a positive move, Big Brother Watch believes that similar movement is required to tackle the overuse of CCTV in schools. The Department for Education’s Protection of Biometric Information of Children in Schools specifically states that parental notification and consent would not be required for the schools to use CCTV. 64 With over 100,000 cameras in schools this is an issue that requires attention. 65
1. RESTRICT SURVEILLANCE POWERS OF LOCAL AUTHORITIES

THE PLEDGE:
The Liberal Democrat Party pledged to "stop councils from spying on people". This is in the context of Local Authorities using the Regulation of Investigatory Powers Act 2000 (RIPA) to use surveillance on local citizens and investigate minor offences.

THE OUTCOME:
On 26 January 2011, the Home Office published a Review of Counter-Terrorism and Security Powers, highlighting local authorities’ use of surveillance to investigate minor offences. The Protection of Freedoms Act 2012 states that all local authority surveillance authorised under the RIPA will have to be approved by a Magistrate. The amendments to RIPA mean that local authorities are no longer able to use any of the three covert investigatory techniques available to them without the approval of the magistrate. The surveillance techniques are as follows:

- Directed surveillance
- The deployment of a Covert Human Intelligence Source (CHIS)
- Accessing communications data

It should however be noted that no such warrants are required for investigations carried out by the police or other public authorities. The Office of Surveillance Commissioners 2013-14 annual report was critical of the lack of knowledge, understanding and training displayed by magistrates regarding RIPA. The report also highlighted the Commissioner’s concerns that officials in public authorities may be wilfully ignoring RIPA by covertly using social media to carry out investigations.

THE CONCLUSION:
Although Big Brother Watch welcomes the requirement of judicial authorisation for local authorities, there are still many fundamental issues with RIPA and its disproportionate use that need to be addressed. These issues include:

- The continued lack of transparency. Although local authorities need to seek the approval of the magistrate, the public still do not know what the surveillance is taking place, how often, for what purpose, or what the outcome is. This data should be made available to the public.
- Anti-terrorism legislation continues to be misused. Judicial authorisation should be a requirement for all authorities wishing to use RIPA and not just for Local Authorities.
- The legislation is out of date. The number of issues with RIPA itself and how it functions calls for an urgent review into the Act rather than continued small amendments.

2. REBALANCE THE US/UK EXTRADITION TREATY

THE PLEDGE:
In 2009, Nick Clegg MP was vocally opposed to what he saw as Gary McKinnon being "hung out to dry by a British Government desperate to appease its American counterparts". As a result the Liberal Democrats pledged to "stop unfair extradition to the US".

THE OUTCOME:
In October 2011 the Independent Review of the United Kingdom’s Extradition Arrangements led by Sir Scott Baker, a former Court of Appeal judge was established. The process involved a review of the controversial Extradition Act 2003 as well as the measures in place between the US and the UK.

Previously, committees including the Home Affairs Select Committee and the Joint Committee on Human Rights (JCHR) have criticised the US-UK Treaty. The JCHR, for example, considered the Trausuantic arrangement to be 'loosided' and something "which allows the US to request the extradition of UK citizens without the requirement to produce evidence of an offence."

In spite of the widespread expectation that the review would find the treaty to be unequal Sir Scott Baker concluded that “the United States/United Kingdom Treaty does not operate in an unbalanced manner”. In June 2014 Lord Hill of Oareford announced the creation of The Committee on Extradition Law, Big Brother Watch looks forward to the Committee’s findings, which are expected to be published by March 2015.

THE CONCLUSION:
The findings of the Baker Review were attacked by a variety of figures. David Davis MP called the report ‘inexplicable’, as “the idea that the UKUS extradition treaty is in any sense symmetrical is in defiance of the facts”. Keith Vaz MP, chairman of the Home Affairs Select Committee, added that he was “concerned that the extradition review has not shed any light on the ease of extradition”. A consultant at Cubism Law, Dan Hyde, warned that the findings would “likely bring calls for the review to be reviewed”.

---


---

BIG BROTHER WATCH
3. DEFEND TRIAL BY JURY

THE PLEDGE:
After their opposition to proposals that would have abolished trial by jury in complex fraud cases, something Simon Hughes MP warned could lead to a ‘two-tier justice system’, the Liberal Democrat Party pledged to ‘defend trial by jury.’

THE OUTCOME:
The Coalition Agreement did not include the defence of trial by jury. Subsequently little has been done to secure the presence of the jury in trials. Although most trials do include a jury, the issue is still contested. This can be seen in the use of secret trials as extended through the Justice and Security Act 2013.

THE CONCLUSION:
As has been warned, criminal cases being heard in secret and without a jury “risks ripping up the very tradition of open justice in the UK”. The consensus is that juries are still an integral part of the British legal system, what JUSTICE call a ‘key constitutional safeguard’. The former Attorney General, Dominic Grieve MP has also stated that trial by jury is an “essential element of the justice system of England and Wales. It is deeply ingrained in our national DNA.”

Big Brother Watch strongly believe in the right to a trial by jury and as the 800th anniversary of Magna Carta approaches, would like to see further action taken to protect this fundamental right.

4. PREVENT THE COLLECTION OF CHILDREN’S BIOMETRIC DATA WITHOUT PERMISSION

THE PLEDGE:
In reaction to the increase in schools using student’s biometric data without their parents’ permission, the Liberal Democrat Party pledged to “stop children being fingerprinted at school without their parents’ permission”.

THE OUTCOME:
The Protection of Freedoms Act 2012 requires schools and further education institutions to:

• Obtain the written consent of parents (or others with main parental responsibility) before processing biometric information from children under the age of 18 years
• Ensure that such information is not processed if a child objects, even where a parent has consented
• Provide reasonable alternative arrangements for pupils who refuse or whose parents do not consent to biometric information being processed

THE CONCLUSION:
The move was welcomed by the Association of School and College Leavers, with the General Secretary Brian Lightman stating that “It’s right that parents give their consent to use biometric data, just as they do for taking photographs.”

Whilst this is a positive move, Big Brother Watch believes that similar movement is required to tackle the overuse of CCTV in schools. The Department for Education’s Protection of Biometric Information of Children in Schools specifically states that parental notification and consent would not be required for the schools to use CCTV. With over 100,000 cameras in schools this is an issue that requires attention.
5. RESTORE THE RIGHT TO PROTEST

THE PLEDGE:
The Liberal Democrat Party pledged to “restore the right to protest by reforming the Public Order Act to safeguard non-violent protest even if it offends”.

THE OUTCOME:
In 2011, the Serious Organised Crime and Police Act 2005 (SOCPA), was repealed. SOCPA restricted peaceful protest within 1km of Parliament Square. However, it was replaced with the Police Reform and Social Responsibility Act 2011 which also imposed tight restrictions on peaceful protest in Parliament Square.

THE CONCLUSION:
A successful campaign to remove the word ‘offensive’ from Section 5 of the Public Order Act 1980 was launched in 2012. The campaigners rightly pointed out that the removal of the word was necessary to protect freedom of speech. Despite this change there has been no further reform to the Act in order to restore the right to non-violent protest.

6. REFORM LIBEL LAWS

THE PLEDGE:
The Liberal Democrat Party pledged to “protect free speech, investigative journalism and academic peer-reviewed publishing through reform of the English and Welsh libel laws”.

THE OUTCOME:
The Defamation Act came into force on 1 January 2014. The Act contains a series of measures to protect freedom of speech. They include:

- Claimants must be able to show that they have suffered serious harm before they can sue for defamation
- Defence for those publishing material on a matter that is in the public interest
- The increase in protection to operators of websites that host user-generated content, provided they comply with the procedure to enable the complainant to resolve disputes directly with the author of the material concerned
- Defence of truth and honest opinion to replace the common law defences of justification and fair comment
- Tightening the test for claims involving those with little connection to England and Wales being brought before the courts to target libel tourism
- Single-publication rule to prevent repeated claims against a publisher about the same material

THE CONCLUSION:
Despite being important and necessary, the new defences in the Defamation Act have not been extended to Northern Ireland, leaving the citizens of that region with fewer and more restricted rights to free speech. The Libel Reform Campaign state that this has:

“Created a loophole in the law. Libel lawyers have already begun touting Belfast to potential litigants as a claimant friendly jurisdiction. This creates uncertainty and confusion for journalists and publishers throughout the United Kingdom.”
5. RESTORE THE RIGHT TO PROTEST

THE PLEDGE:
The Liberal Democrat Party pledged to “restore the right to protest by reforming the Public Order Act to safeguard non-violent protest even if it offends”.

THE OUTCOME:
In 2011, the Serious Organised Crime and Police Act 2005 (SOCPA), was repealed. SOCPA restricted peaceful protest within 1km of Parliament Square. However, it was replaced with the Police Reform and Social Responsibility Act 2011 which also imposed tight restrictions on peaceful protest in Parliament Square.

THE CONCLUSION:
A successful campaign to remove the word ‘offensive’ from Section 5 of the Public Order Act 1980 was launched in 2012. The campaigners rightly pointed out that the removal of the word was necessary to protect freedom of speech. Despite this change there has been no further reform to the Act in order to restore the right to non-violent protest.

6. REFORM LIBEL LAWS

THE PLEDGE:
The Liberal Democrat Party pledged to “protect free speech, investigative journalism and academic peer-reviewed publishing through reform of the English and Welsh libel laws”.

THE OUTCOME:
The Defamation Act came into force on 1 January 2014. The Act contains a series of measures to protect freedom of speech. They include:

- Claimants must be able to show that they have suffered serious harm before they can sue for defamation
- Defence for those publishing material on a matter that is in the public interest
- The increase in protection to operators of websites that host user-generated content, provided they comply with the procedure to enable the complainant to resolve disputes directly with the author of the material concerned
- Defence of truth and honest opinion to replace the common law defences of justification and fair comment

- Tightening the test for claims involving those with little connection to England and Wales being brought before the courts to target libel tourism
- Single-publication rule to prevent repeated claims against a publisher about the same material

THE CONCLUSION:
Despite being important and necessary, the new defences in the Defamation Act have not been extended to Northern Ireland, leaving the citizens of that region with fewer and more restricted rights to free speech. The Libel Reform Campaign state that this has:

“Created a loophole in the law. Libel lawyers have already begun touting Belfast to potential litigants as a claimant friendly jurisdiction. This creates uncertainty and confusion for journalists and publishers throughout the United Kingdom.”
7. **ABOLISH ID CARDS AND INCREASE THE NUMBER OF POLICE OFFICERS**

**THE PLEDGE:**
The Liberal Democrats pledged to “scrap intrusive identity cards and have more police instead”.

**THE OUTCOME:**
ID cards were scrapped in 2010 under the *Identity Documents Act* which repealed the *Identity Card Act 2006*.

The Deputy Prime Minister, Nick Clegg MP stated that:

“By taking swift action to scrap it, we are making it clear that this government won’t sacrifice people’s liberty… Cancelling the scheme and abolishing the National Identity Register is a major step in dismantling the surveillance state.”

The Liberal Democrats were unable to meet their pledge to increase police levels. They have been hindered by budget cuts, In March 2010 there were 244,497 FTE staff working in the 43 police forces in England and Wales.

By March 2014 this number had dropped to 209,362. There has also been a decrease in frontline police officers from 143,734 in 2010 to 127,909 in 2014. A drop of 15,825 or 11%.

**THE CONCLUSION:**
Big Brother Watch welcomed the abolition of ID cards the scheme would have enabled government departments and companies to share masses of individuals’ personal data; allowing the state to continuously track every British citizen’s movements is a process which Big Brother Watch wholly oppose.

8. **SCRAP PLAN FOR SECOND GENERATION EPASSPORTS**

**THE PLEDGE:**
The Liberal Democratic Party stated that it would “scrap plans for expensive, unnecessary new passports with additional biometric data”.

**THE OUTCOME:**
Passports that contain biometric data, known as ePassports, have existed since 2006. In the UK they include information such as an image of the holder’s face and ‘relevant biographical details’.

The Labour Government had intended to introduce second generation ePassports, that would include fingerprint data, however these plans were scrapped as part of the Coalition Agreement.

**THE CONCLUSION:**
Big Brother Watch welcomes the Coalition Government’s decision to scrap plans for second generation ePassports. Inclusion of additional biometric data would be an unnecessary collection of an individuals’ personal data.
7. ABOLISH ID CARDS AND INCREASE THE NUMBER OF POLICE OFFICERS

THE PLEDGE:
The Liberal Democrats pledged to “scrap intrusive identity cards and have more police instead”.

THE OUTCOME:
ID cards were scrapped in 2010 under the Identity Documents Act which repealed the Identity Card Act 2006. The Deputy Prime Minister, Nick Clegg MP stated that: “By taking swift action to scrap it, we are making it clear that this government won’t sacrifice people’s liberty... Cancelling the scheme and abolishing the National Identity Register is a major step in dismantling the surveillance state.”

The Liberal Democrats were unable to meet their pledge to increase police levels. They have been hindered by budget cuts, In March 2010 there were 244,497 FTE staff working in the 43 police forces in England and Wales. By March 2014 this number had dropped to 209,362. There has also been a decrease in frontline police officers from 143,734 in 2010 to 127,909 in 2014. A drop of 15,825 or 11%.

THE CONCLUSION:
Big Brother Watch welcomed the abolition of ID cards the scheme would have enabled government departments and companies to share masses of individuals’ personal data; allowing the state to continuously track every British citizen’s movements is a process which Big Brother Watch wholly oppose.

8. SCRAP PLAN FOR SECOND GENERATION EPASSPORTS

THE PLEDGE:
The Liberal Democratic Party stated that it would “scrap plans for expensive, unnecessary new passports with additional biometric data”.

THE OUTCOME:
Passports that contain biometric data, known as ePassports, have existed since 2006. In the UK they include information such as an image of the holder’s face and ‘relevant biographical details’. The Labour Government had intended to introduce second generation ePassports, that would include fingerprint data, however these plans were scrapped as part of the Coalition Agreement.

THE CONCLUSION:
Big Brother Watch welcomes the Coalition Government’s decision to scrap plans for second generation ePassports. Inclusion of additional biometric data would be an unnecessary collection of an individuals’ personal data.
9. PREVENT AN INCREASE IN NEW OFFENCES

THE PLEDGE:
The Liberal Democrat Party stated that it would “halt the increase in new offences with the creation of a ‘stop unit’ in the Cabinet Office”.

THE OUTCOME:
This pledge did not feature in the Coalition Agreement. A ‘stop unit’ was never created.

THE CONCLUSION:
Under the Coalition Government there has not been an excessive increase in new offences, however the creation of a ‘stop unit’ in the Cabinet Office would be welcomed.

10. PREVENT STORAGE OF EMAIL AND INTERNET RECORDS

THE PLEDGE:
The Liberal Democrats pledged to “end plans to store your email and internet records without good cause”.

THE OUTCOME:
In 2013, the Deputy Prime Minister made his opposition to the Draft Communications Data Bill clear when he blocked its progress, stating that “It’s certainly not going to happen with Liberal Democrats in government”. This Bill, dubbed the Snooper’s Charter, planned to include the storage of:

- All details of online communication in the UK including time, duration, originator and recipient of a communication and the location of the device used to communicate
- All Britons’ web browsing history and details of messages sent on social media and email
- Voice calls over the internet and gaming as well as phone calls

The persistent opposition to the Bill led to its notable absence in the Queen’s speech in 2013 and 2014. However, the legislating of the emergency Data Retention and Investigatory Powers (DRIP) Act saw widespread Liberal Democrat support, despite John McDonnell MP stating that DRIP is “the foot in the door towards bringing back the communications legislation that was proposed previously”.

THE CONCLUSION:
Whilst the Draft Communications Data Bill was “kicked into the long grass after Nick Clegg withdrew support,” others in the Government continue to push for the Bill. In a speech to the Royal United Services Institute, the Home Secretary, Theresa May MP, stated:

“We need to address declining capabilities in communications data. There is a need to get out there more generally the importance of intelligence in fighting all of these national security threats... People talk about national security versus civil liberties, but you can only enjoy your liberty if you have security.”

The Liberal Democrats failed to curb the passing of the Data Retention and Investigatory Powers Act. Whilst DRIP’s sunset clause comes with the promise of a full and proper review into RIPA and the government’s interception and data retention laws, there are still serious concerns regarding whether or not the result of these reviews will lead to an appropriate balance between security, privacy and civil liberties. A further concern is Clause 17 of the Counter-Terrorism and Security Bill, which allows for the retention of IP addresses. It is worrying that is being classed as ‘fast-track’ legislation and will amend the above emergency legislation. It is vital that MPs and Peers are given the proper time to scrutinise any new surveillance powers.

84. The Liberal Democrat Manifesto 2010, p.94
85. BBC, Nick Clegg: No ‘web snooping’ bill while Lib Dems in government: http://www.bbc.co.uk/news/uk-politics-22292474
9. PREVENT AN INCREASE IN NEW OFFENCES

THE PLEDGE:
The Liberal Democrat Party stated that it would “halt the increase in new offences with the creation of a ‘stop unit’ in the Cabinet Office”.83

THE OUTCOME:
This pledge did not feature in the Coalition Agreement. A ‘stop unit’ was never created.

THE CONCLUSION:
Under the Coalition Government there has not been an excessive increase in new offences, however the creation of a ‘stop unit’ in the Cabinet Office would be welcomed.

10. PREVENT STORAGE OF EMAIL AND INTERNET RECORDS

THE PLEDGE:
The Liberal Democrats pledged to “end plans to store your email and internet records without good cause”.84

THE OUTCOME:
In 2013, the Deputy Prime Minister made his opposition to the Draft Communications Data Bill clear when he blocked its progress, stating that “It’s certainly not going to happen with Liberal Democrats in government”.85

This Bill, dubbed the Snooper’s Charter, planned to include the storage of:

- All details of online communication in the UK including time, duration, originator and recipient of a communication and the location of the device used to communicate
- All Britons’ web browsing history and details of messages sent on social media and email
- Voice calls over the internet and gaming as well as phone calls

The persistent opposition to the Bill led to its notable absence in the Queen’s speech in 2013 and 2014. However, the legislating of the emergency Data Retention and Investigatory Powers (DRIP) Act saw widespread Liberal Democrat support, despite John McDonnell MP stating that DRIP is “the foot in the door towards bringing back the communications legislation that was proposed previously”86.

THE CONCLUSION:
Whilst the Draft Communications Data Bill was “kicked into the long grass after Nick Clegg withdrew support,” others in the Government continue to push for the Bill.87 In a speech to the Royal United Services Institute, the Home Secretary, Theresa May MP, stated:

“We need to address declining capabilities in communications data. There is a need to get out there more generally the importance of intelligence in fighting all of these national security threats... People talk about national security versus civil liberties, but you can only enjoy your liberty if you have security.”88

The Liberal Democrats failed to curb the passing of the Data Retention and Investigatory Powers Act. Whilst DRIP’s sunset clause comes with the promise of a full and proper review into RIPA and the government’s interception and data retention laws, there are still serious concerns regarding whether or not the result of these reviews will lead to an appropriate balance between security, privacy and civil liberties.

A further concern is Clause 17 of the Counter-Terrorism and Security Bill, which allows for the retention of IP addresses. It is worrying that is being classed as ‘fast-track’ legislation and will amend the above emergency legislation. It is vital that MPs and Peers are given the proper time to scrutinise any new surveillance powers.

85. BBC, Nick Clegg: No ‘web snooping’ bill while Lib Dems in government: http://www.bbc.co.uk/news/uk-politics-22292474
88. Ibid.

BIG BROTHER WATCH
THE PLEDGE:
The Liberal Democrat Party pledged to “remove innocent people from police DNA database and stop storing DNA from innocent people and children in the future”.

THE OUTCOME:
The Protection of Freedoms Act 2012 included measures to remove the DNA records of more than one million innocent adults and children. The Act enables DNA samples of convicted individuals to stay on the database for three years. This is extendable by a further three years by a court order.

In 2013, Criminal Information Minister Lord Taylor of Holbeach said:

“Over 1.7 million DNA profiles taken from innocent people and from children have been removed from the DNA database. The destruction of all 7,753,000 DNA samples is a significant step to protect the genetic privacy of people in the United Kingdom.”

THE CONCLUSION:
Although the deletion of more than 1.7 million DNA profiles taken from innocent people and children is a good first step, there are still some issues that the Protection of Freedoms Act did not address. These include:

- Indefinite retention of DNA profiles from adults who have committed a minor offence and children who have committed more than one minor offence, is still disproportionate
- Collection of DNA on arrest for all recordable offences even if DNA is not relevant to solving the crime is unnecessary and expensive
- The length of time that the Police National Computer records are retained for innocent people and those who committed minor offences is still unclear

More can still be done to ensure that only the most necessary samples are kept on the National DNA database.

Big Brother Watch maintain the position that the wholesale implementation of the ‘Scottish Model’ for DNA retention would be preferable to the existing arrangements. Whilst the Coalition has made some changes it is important that they continue to reform retention policies to bring them in line with the fairer and less permissive system in Scotland.

---

THE PLEDGE:
The Liberal Democrats pledged to “scrap the intrusive ContactPoint database which is intended to hold the details of every child in England”.

THE OUTCOME:
On 22 July 2010, the Children and Families Minister, Tim Loughton MP, confirmed that ContactPoint would be shut down on 6 August 2010. He stated that “I wasn’t wrong to switch off this flawed child register. ContactPoint failed to protect our children – it prioritised data input over social work”.

THE CONCLUSION:
ContactPoint was unnecessary, flawed, dangerously unstable and a violation of the privacy of 11 million children.

---

92. Ibid.
11. REMOVE INNOCENT PEOPLE’S DNA FROM POLICE DATABASE

**THE PLEDGE:**
The Liberal Democrat Party pledged to “remove innocent people from police DNA database and stop storing DNA from innocent people and children in the future”.

**THE OUTCOME:**
The Protection of Freedoms Act 2012 included measures to remove the DNA records of more than one million innocent adults and children. The Act enables DNA samples of convicted individuals to stay on the database for three years. This is extendable by a further three years by a court order.

In 2013, Criminal Information Minister Lord Taylor of Holbeach said:

“Over 1.7 million DNA profiles taken from innocent people and from children have been removed from the DNA database. The destruction of all 7,753,000 DNA samples is a significant step to protect the genetic privacy of people in the United Kingdom.”

**THE CONCLUSION:**
Although the deletion of more than 1.7 million DNA profiles taken from innocent people and children is a good first step, there are still some issues that the Protection of Freedoms Act did not address. These include:

- Indefinite retention of DNA profiles from adults who have committed a minor offence and children who have committed more than one minor offence, is still disproportionate
- Collection of DNA on arrest for all recordable offences even if DNA is not relevant to solving the crime is unnecessary and expensive
- The length of time that the Police National Computer records are retained for innocent people and those who committed minor offences is still unclear

More can still be done to ensure that only the most necessary samples are kept on the National DNA database.

Big Brother Watch maintain the position that the wholesale implementation of the ‘Scottish Model’ for DNA retention would be preferable to the existing arrangements. Whilst the Coalition has made some changes it is important that they continue to reform retention policies to bring them in line with the fairer and less permissive system in Scotland.

---


92. Ibid.

---

12. SCRAP THE CONTACTPOINT DATABASE

**THE PLEDGE:**
The Liberal Democrats pledged to “scrap the intrusive ContactPoint database which is intended to hold the details of every child in England”.

**THE OUTCOME:**
On 22 July 2010, the Children and Families Minister, Tim Loughton MP, confirmed that ContactPoint would be shut down on 6 August 2010. He stated that “I wasn’t wrong to switch off this flawed child register. ContactPoint failed to protect our children – it prioritised data input over social work”.

**THE CONCLUSION:**
ContactPoint was unnecessary, flawed, dangerously unstable and a violation of the privacy of 11 million children.

---


13. SCRAP CONTROL ORDERS

THE PLEDGE:
The Liberal Democrat Party pledged that it would “scrap control orders, which can use secret evidence to place people under house arrest,” the Liberal Democrats pledged. 98

THE OUTCOME:
According to Chris Huhne MP, control orders were a “violation of fundamental rights and an expensive failure to boot.” 99 They were scrapped on 26 January 2014. Control orders were replaced with Terrorism Prevention and Investigation Measures (TPIMs) which resembles control orders in most respects, however, there are some notable differences:

- Their maximum two-year duration
- The inability to relocate TPIM subjects to places remote from their alleged associates
- Less onerous conditions, especially as regards search powers, overnight residence and the use of electronic communications

In November 2014 the Counter-Terrorism and Security Bill was announced. It proposed the reintroduction of relocation. At the same time the level of evidence needed to impose relocation is to be raised to a “reasonable balance of probabilities”. 100

THE CONCLUSION:
Commenting on TIPMs the Joint Committee on Human Rights report states:

“TPIMs are functionally punitive measures enforced on individuals and families who have never been convicted of any crime. TPIMs do not keep us safer because those who want to abscond will. These measures are undemocratic and poor public policy.” 101

This new system is in many ways simply a rebranding of Control Orders. Many of the old problems still remain. The issue that these orders do not need to be part of a wider and ongoing criminal investigation continues to be highly troubling. Whilst there is now a requirement to renew the orders after two years this remains a highly repressive measure.

13. **SCRAP CONTROL ORDERS**

**THE PLEDGE:**

The Liberal Democrat Party pledged that it would “scrap control orders, which can use secret evidence to place people under house arrest,” the Liberal Democrats pledged. 99

**THE OUTCOME:**

According to Chris Huhne MP, control orders were a “violation of fundamental rights and an expensive failure to boot.” 96 They were scrapped on 26 January 2014. Control orders were replaced with Terrorism Prevention and Investigation Measures (TPIMs) which resembles control orders in most respects, however, there are some notable differences:

- Their maximum two-year duration
- The inability to relocate TPIM subjects to places remote from their alleged associates
- Less onerous conditions, especially as regards search powers, overnight residence and the use of electronic communications

In November 2014 the Counter-Terrorism and Security Bill was announced. It proposed the reintroduction of relocation. At the same time the level of evidence needed to impose relocation is to be raised to a “reasonable balance of probabilities”. 97

**THE CONCLUSION:**

Commenting on TPIMs the Joint Committee on Human Rights report states:

“TPIMs are functionally punitive measures enforced on individuals and families who have never been convicted of any crime. TPIMs do not keep us safer because those who want to abscond will. These measures are undemocratic and poor public policy.” 98

98. Lord Carlile, a former Independent Reviewer of Terrorism Legislation, welcomed the change stating that the 14 day limit had proved ‘perfectly sufficient’. 101

14. **REDUCE MAXIMUM PERIOD OF PRE-CHARGE DETENTION TO 14-DAY DETENTION**

**THE PLEDGE:**

The Liberal Democrat Party pledged to “reduce the maximum period of pre-charge detention to 14 days”. 100

**THE OUTCOME:**

The Terrorism Act 2000 extended the length of time a suspect could be held before being charged with committing a crime from 14 days to 28 days. The process was subject to a review every 6 months. In July 2010 the 28-day period was renewed for a six-month period and subsequently allowed to expire in January 2011. The limit reverted to 14 days and the Protection of Freedoms Act 2012 permanently reduced the pre-charge detention period to a maximum of 14 days.

**THE CONCLUSION:**

“TPIMs are functionally punitive measures enforced on individuals and families who have never been convicted of any crime. TPIMs do not keep us safer because those who want to abscond will. These measures are undemocratic and poor public policy.” 98

This new system is in many ways simply a rebranding of Control Orders. Many of the old problems still remain. The issue that these orders do not need to be part of a wider and ongoing criminal investigation continues to be highly troubling. Whilst there is now a requirement to renew the orders after two years this remains a highly repressive measure.
**The Labour Party Manifesto only mentions civil liberties once.** This is in a section entitled ‘using technology to cut crime’ in which the Labour Party stated that they were “proud of [their] record on civil liberties” and cited the two following examples of how they had protected them:

- Taking the DNA profiles of children ‘off the database’
- Tightening the rules around surveillance

The section included three major pledges:

- Enable more CCTV cameras to be installed, stating that they had “brought in a new power for people to petition their local authority for more CCTV”
- Offer the “new biometric ID scheme… to an increasing number of British citizens”
- Retention of DNA profiles for those arrested but not convicted for six years

**Post 2010 General Election**

**Outside Parliament: 2010-2012**

In his first speech as leader, **Ed Miliband MP argued** that he would not let the Coalition Government “take ownership of the British tradition of liberty.” He stated that the broad use of anti-terrorism powers, for instance 90-day detention, had been wrong. However, he still supported the previous Labour Government’s stance on CCTV and DNA, referring to them as ‘important things’.

In his 2010 speech to Labour Party Conference, as **Shadow Justice Secretary, Jack Straw MP** attacked the Coalition’s decision to cut the use of both CCTV and DNA technology. He argued that only criminals would benefit from ‘this madness,’ and there would be “greater freedom for the criminal, less liberty for the law abiding”.

He ended the speech by arguing that these measures represented some of the Liberals’ ‘most dangerous’ policies on crime.

This continued focus on the use of CCTV and DNA technology to fight crime was echoed by **Ed Balls MP**, the then Shadow Home Secretary, who claimed that people wanted more CCTV because “they want to feel safe”. However, he too conceded that 90-day detention was a “step too far”.

**Outside Parliament: 2012-2014**

In his speech to the 2012 Labour Party Conference **Sadiq Khan MP** stated that Labour was “the party of open and fair justice and civil liberties.” **Labour** has yet to fully meet this claim. Several speeches made by the Shadow Home Secretary, **Yvette Cooper MP**, highlight the changeable position of the Labour Party when it comes to balancing security and privacy and civil liberties.

In July 2013 **Cooper argued** that Coalition decisions such as restricting DNA use were “not in the interests of fighting crime or protecting security”. Yet, in the same speech she welcomed the restrictions that the Government had placed on the use of RIPA by local authorities.

In March 2014, in a speech at Demos, **Cooper argued** for the strengthening of the Intelligence and Security Committee (ISC) to allow it to be a more effective oversight body. She also argued for an “overhaul of the system of independent oversight commissioners”.

She hoped that the way in which they work would become more public facing. Citing the approach **David Anderson QC** has taken in his role as the Independent Reviewer of Terrorism Legislation.

The result of giving the commissioner system a higher profile would be that members of the public would gain a better understanding of what it is that the intelligence services do, as well as how the oversight mechanisms function. This will make it easier for the public to make judgments about the effectiveness of the system.

She ended by recommending that the legal framework should be reconsidered; recognising that the **Regulation of Investigatory Powers Act 2000** was “introduced before the explosion of online communications and social media”.

The Shadow Home Secretary recognised privacy was a growing issue, especially when it comes to how the private sector use data and how they protect their customers’ personal information.

**In Parliament**

In the debate around the **Draft Communications Data Bill** the party’s interventions were minimal. The Shadow Home Secretary did, however, rule out helping the Conservatives pass the Bill without the support of their Coalition partners. She argued that the Government “needed to urgently rethink this legislation”.

It is worth noting that Labour’s opposition to these measures may not be entirely based on concerns over civil liberties. In an interview with the New Statesman **Cooper appeared** to challenge the issue by raising concerns of funding, stating “if you need additional services, for example, do you have the necessary resources to deliver it?”

---

103. Y. Cooper, The role for Government in seeking to ensure people’s liberty and security: Speech to Demos: http://www.yvettecooper.com/the_role_for_government_in_seeking_to_ensure_people_s_liberty_and_security
105. Ibid.
106. H. Cooper, The role for Government in seeking to ensure people’s liberty and security: Speech to Demos: http://www.yvettecooper.com/the_role_for_government_in_seeking_to_ensure_people_s_liberty_and_security
107. Y. Cooper, The role for Government in seeking to ensure people’s liberty and security: Speech to Demos: http://www.yvettecooper.com/the_role_for_government_in_seeking_to_ensure_people_s_liberty_and_security
108. Ibid.
109. Ibid.
110. Ibid.
111. Ibid.
112. Ibid.
113. Ibid.
114. Ibid.
115. Ibid.
116. Ibid.
117. Ibid.
118. Ibid.
THE 2010 LABOUR PARTY MANIFESTO

The Labour Party Manifesto only mentions civil liberties once. This is in a section entitled ‘using technology to cut crime’ in which the Labour Party stated that they were “proud of [their] record on civil liberties”102 and cited the two following examples of how they had protected them:

• Taking the DNA profiles of children ‘off the database’
• Tightening the rules around surveillance

The section included three major pledges:

• Enable more CCTV cameras to be installed, stating that they had “brought in a new power for people to petition their local authority for more CCTV”103
• Offer the “new biometric ID scheme… to an increasing number of British citizens”104
• Retention of DNA profiles for those arrested but not convicted for six years

POST 2010 GENERAL ELECTION

OUTSIDE PARLIAMENT: 2010-2012

In his first speech as leader, Ed Miliband MP argued that he would not let the Coalition Government “take ownership of the British tradition of liberty”.105 He stated that the broad use of anti-terrorism powers, for instance 90-day detention, had been wrong. However, he still supported the previous Labour Government’s stance on CCTV and DNA, referring to them as ‘important things’.106

His in 2010 speech to Labour Party Conference, as Shadow Justice Secretary, Jack Straw MP attacked the Coalition’s decision to cut the use of both CCTV and DNA technology. He argued that only criminals would benefit from ‘this madness,’ and there would be ‘greater freedom for the criminal, less liberty for the law abiding”.107, 108 He ended the speech by arguing that these measures represented some of the Liberals’ ‘most dangerous’ policies on crime.109 This continued focus on the use of CCTV and DNA technology to fight crime was echoed by Ed Balls MP, the then Shadow Home Secretary, who claimed that people wanted more CCTV because “they want to feel safe”.110 However, he too conceded that 90-day detention was a “step too far”.111

IN PARLIAMENT

In the debate around the Draft Communications Data Bill the party’s interventions were minimal. The Shadow Home Secretary did, however, rule out helping the Conservatives pass the Bill without the support of their Coalition partners. She argued that the Government “needed to urgently rethink this legislation”.112 Yet, in the same speech she welcomed the restrictions that the Government had placed on the use of RIPA by local authorities. In March 2014, in a speech at Demos, Cooper argued for the strengthening of the Intelligence and Security Committee (ISC) to allow it to be a more effective oversight body. She also argued for an “overhaul of the system of independent oversight commissioners”.113 She hoped that the way in which they work would become more public facing. Citing the approach David Anderson QC has taken in his role as the Independent Reviewer of Terrorism Legislation.

The result of giving the commissioner system a higher profile would be that members of the public would gain a better understanding of what it is that the intelligence services do, as well as how the oversight mechanisms function. This will make it easier for the public to make judgements about the effectiveness of the system.

She ended by recommending that the legal framework should be reconsidered; recognising that the Regulation of Investigatory Powers Act 2000 was “introduced before the explosion of online communications and social media”.114 The Shadow Home Secretary recognised that privacy was a growing issue, especially when it comes to how the private sector use data and how they protect their customers’ personal information.115

BIG BROTHER WATCH

OUTSIDE PARLIAMENT: 2012-2014

In his speech to the 2012 Labour Party Conference Sadiq Khan MP stated that Labour was “the party of open and fair justice and civil liberties”.115 Labour has yet to fully meet this claim. Several speeches made by the Shadow Home Secretary, Yvette Cooper MP, highlight the changeable position of the Labour Party when it comes to balancing security and privacy and civil liberties.

In July 2013 Cooper argued that Coalition decisions such as restricting DNA use were “not in the interests of fighting crime or protecting security”.116 Yet, in the same speech she welcomed the restrictions that the Government had placed on the use of RIPA by local authorities.

In March 2014, in a speech at Demos, Cooper argued for the strengthening of the Intelligence and Security Committee (ISC) to allow it to be a more effective oversight body. She also argued for an “overhaul of the system of independent oversight commissioners”.113 She hoped that the way in which they work would become more public facing. Citing the approach David Anderson QC has taken in his role as the Independent Reviewer of Terrorism Legislation.

The result of giving the commissioner system a higher profile would be that members of the public would gain a better understanding of what it is that the intelligence services do, as well as how the oversight mechanisms function. This will make it easier for the public to make judgements about the effectiveness of the system.

She ended by recommending that the legal framework should be reconsidered; recognising that the Regulation of Investigatory Powers Act 2000 was “introduced before the explosion of online communications and social media”.114 The Shadow Home Secretary recognised that privacy was a growing issue, especially when it comes to how the private sector use data and how they protect their customers’ personal information.115

115. Ibid p.54
116. Ibid

Framing the argument with alternatives to the privacy argument was Labour’s stance during the Data Retention and Investigatory Powers Bill (DRIP) debate also. It is worth noting that when the Shadow Home Secretary mentioned the importance of privacy and civil liberties, it was simply to reinforce Labour’s disapproval of the parliamentary process used to rush through legislation, that it was “only debated behind closed doors”119, rather than emphasising their concerns in this respect. Cooper stated:

“It has been left until the final full week of Parliament before the recess and must be published and debated in both Houses in a week, and it relates to laws and technologies that are complex and controversial. They reflect the serious challenge of how to sustain both liberty and security, and privacy and safety in a democracy. This is therefore not the way in which such legislation should be done. Let me be clear that its last-minute nature undermines trust not only in the Government’s intentions, but also in the vital work of the police and agencies.”120

The work against DRIPA by Tom Watson MP is also notable. His work in getting DRIPA in the public domain as early as possible was commendable. By doing so he ensured that the process as well as the content of the legislation, were placed under scrutiny.

THE CONCLUSION

Since 2010, Labour has failed to position itself properly in the debate around civil liberties. There have been limited reversals of previous policies, for example the recognition that 90-day detention was extremely excessive and a violation of human rights.

Big Brother Watch is encouraged by Labour’s calls for the reform of the Intelligence and Security Committee, renewed scrutiny of RIPA, and a proper debate on the balance between privacy and security to take place in December 2016. Their amendments to DRIPA are also welcome. However Big Brother Watch believe that a large section of the Labour Party still place far too great an emphasis on the use of technologies such as CCTV and DNA as benefits to liberty and fail to strike an appropriate balance between crime prevention and civil liberties.

120. Ibid
Framing the argument with alternatives to the privacy argument was Labour’s stance during the Data Retention and Investigatory Powers Bill (DRIP) debate also. It is worth noting that when the Shadow Home Secretary mentioned the importance of privacy and civil liberties, it was simply to reinforce Labour’s disapproval of the parliamentary process used to rush through legislation, that it was “only debated behind closed doors”\(^\text{119}\), rather than emphasising their concerns in this respect. Cooper stated:

“It has been left until the final full week of Parliament before the recess and must be published and debated in both Houses in a week, and it relates to laws and technologies that are complex and controversial. They reflect the serious challenge of how to sustain both liberty and security, and privacy and safety in a democracy. This is therefore not the way in which such legislation should be done. Let me be clear that its last-minute nature undermines trust not only in the Government’s intentions, but also in the vital work of the police and agencies.”\(^\text{119}\)

The work against DRIPA by Tom Watson MP is also notable. His work in getting DRIPA in the public domain as early as possible was commendable. By doing so he ensured that the process as well as the content of the legislation, were placed under scrutiny.

THE CONCLUSION

Since 2010, Labour has failed to position itself properly in the debate around civil liberties. There have been limited reversals of previous policies, for example the recognition that 90-day detention was extremely excessive and a violation of human rights.

Big Brother Watch is encouraged by Labour’s calls for the reform of the Intelligence and Security Committee, renewed scrutiny of RIPA, and a proper debate on the balance between privacy and security to take place in December 2016. Their amendments to DRIPA are also welcome. However Big Brother Watch believe that a large section of the Labour Party still place far too great an emphasis on the use of technologies such as CCTV and DNA as benefits to liberty and fail to strike an appropriate balance between crime prevention and civil liberties.
This section addresses the commitments made in the Coalition Agreement by the Conservative and Liberal Democrat Parties following the 2010 General Election.

### THE CONSERVATIVE PARTY

<table>
<thead>
<tr>
<th>Pledge</th>
<th>Coalition Policy</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scrap ID Cards, the National Identity Register and the ContactPoint Database.</td>
<td></td>
<td>Identity Documents Act 2010 - Abolished ID Cards and the National Identity Register. ContactPoint was shut down in August 2010.</td>
</tr>
<tr>
<td>Strengthen the Information Commissioner’s Powers.</td>
<td>Partially</td>
<td>Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 – Increased fines and powers available to ICO.</td>
</tr>
<tr>
<td>Review Libel Laws.</td>
<td>Yes</td>
<td>Higher thresholds for libel cases to be brought and extended protections for publishers. However Northern Ireland is not covered by the legislation.</td>
</tr>
<tr>
<td>Remove the DNA of innocent people from National DNA Database (NDNAD).</td>
<td>Partially</td>
<td>Protection of Freedoms Act 2012 – Led to the removal of 1.7m DNA profiles taken from innocent people and children from the NDNAD. However the Scottish DNA model was not established.</td>
</tr>
<tr>
<td>Reform Criminal Records Bureau checks.</td>
<td>Yes</td>
<td>The CRB and Independent Safeguarding Authority merged to create the Disclosure and Barring Service.</td>
</tr>
</tbody>
</table>

### THE LIBERAL DEMOCRAT PARTY

<table>
<thead>
<tr>
<th>Pledge</th>
<th>Coalition Policy</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Make Privacy Impact Assessments (PIAs) Mandatory for Data Sharing Proposals.</td>
<td>No</td>
<td>There have been no attempts to make PIAs compulsory.</td>
</tr>
<tr>
<td>Prevent the use of Anti-Terrorism Laws for minor incidents.</td>
<td>Partially</td>
<td>Protection of Freedoms Act 2012 – Local authorities are now required to apply for a magistrates warrant for any surveillance to be undertaken under RIPA 2000. This does not apply to other public authorities where internal authorisation is still the norm.</td>
</tr>
<tr>
<td>Scrutiny of New Powers of Data-Sharing.</td>
<td>No</td>
<td>No progress, the scrutiny of new data sharing proposals remains largely similar to previous systems.</td>
</tr>
<tr>
<td>Create a UK Bill of Rights.</td>
<td>Partially</td>
<td>A Commission on a Bill of Rights established in March 2011 to recommend a course of action. However the Commission’s final report, in December 2012, showed that they had failed to reach a consensus.</td>
</tr>
<tr>
<td>Restrict Surveillance Powers of Local Authorities.</td>
<td>Yes</td>
<td>Protection of Freedoms Act 2012 – Local Authorities are now required to apply for a Magistrates Warrant for any surveillance to be undertaken under RIPA 2000.</td>
</tr>
<tr>
<td>Rebalance the US/UK Extradition Treaty.</td>
<td>Yes</td>
<td>Committee on Extradition Law established to reassess the fairness of the treaty.</td>
</tr>
</tbody>
</table>

### BIG BROTHER WATCH

- **Pledge:** Make Privacy Impact Assessments (PIAs) Mandatory for Data Sharing Proposals.
  - **Coalition Policy:** No
  - **Outcome:** There have been no attempts to make PIAs compulsory.
- **Pledge:** Prevent the use of Anti-Terrorism Laws for minor incidents.
  - **Coalition Policy:** Partially
  - **Outcome:** Protection of Freedoms Act 2012 – Local authorities are now required to apply for a magistrates warrant for any surveillance to be undertaken under RIPA 2000. This does not apply to other public authorities where internal authorisation is still the norm.
- **Pledge:** Scrutiny of New Powers of Data-Sharing.
  - **Coalition Policy:** No
  - **Outcome:** No progress, the scrutiny of new data sharing proposals remains largely similar to previous systems.
- **Pledge:** Create a UK Bill of Rights.
  - **Coalition Policy:** Partially
  - **Outcome:** A Commission on a Bill of Rights established in March 2011 to recommend a course of action. However the Commission’s final report, in December 2012, showed that they had failed to reach a consensus.
- **Pledge:** Restrict Surveillance Powers of Local Authorities.
  - **Coalition Policy:** Yes
  - **Outcome:** Protection of Freedoms Act 2012 – Local Authorities are now required to apply for a Magistrates Warrant for any surveillance to be undertaken under RIPA 2000.
- **Pledge:** Rebalance the US/UK Extradition Treaty.
  - **Coalition Policy:** Yes
  - **Outcome:** Committee on Extradition Law established to reassess the fairness of the treaty.
This section addresses the commitments made in the Coalition Agreement by the Conservative and Liberal Democrat Parties following the 2010 General Election.

### THE CONSERVATIVE PARTY

<table>
<thead>
<tr>
<th>Pledge</th>
<th>Coalition Policy</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scrap ID Cards, the National Identity Register and the ContactPoint Database.</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Strengthen the Information Commissioner’s Powers.</td>
<td></td>
<td>Partially</td>
</tr>
<tr>
<td>Curtail Powers of Entry.</td>
<td></td>
<td>Partially</td>
</tr>
<tr>
<td>Review Libel Laws.</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Remove the DNA of innocent people from National DNA Database (NDNAD).</td>
<td></td>
<td>Partially</td>
</tr>
<tr>
<td>Reform Criminal Records Bureau checks.</td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>

### THE LIBERAL DEMOCRAT PARTY

<table>
<thead>
<tr>
<th>Pledge</th>
<th>Coalition Policy</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restrict Surveillance Powers of Local Authorities.</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Rebalance the US/UK Extradition Treaty.</td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Pledge</th>
<th>Coalition Policy</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Make Privacy Impact Assessments (PIAs) Mandatory for Data Sharing Proposals.</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Prevent the use of Anti-Terrorism Laws for minor incidents.</td>
<td></td>
<td>Partially</td>
</tr>
<tr>
<td>Scrutiny of New Powers of Data-Sharing.</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Create a UK Bill of Rights.</td>
<td></td>
<td>Partially</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Pledge</th>
<th>Coalition Policy</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Documents Act 2010 - Abolished ID Cards and the National Identity Register. ContactPoint was shut down in August 2010.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 – Increased fines and powers available to ICO.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protection of Freedoms Act 2012 – Initiated review of powers of entry by all Government departments. The review published in December 2014; however the process left work still to be done.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Higher thresholds for libel cases to be brought and extended protections for publishers. However Northern Ireland is not covered by the legislation.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protection of Freedoms Act 2012 – Led to the removal of 1.7m DNA profiles taken from innocent people and children from the NDNAD. However the Scottish DNA model was not established.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The CRB and Independent Safeguarding Authority merged to create the Disclosure and Barring Service.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Pledge</th>
<th>Coalition Policy</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection of Freedoms Act 2012 – Local authorities are now required to apply for a magistrates warrant for any surveillance to be undertaken under RIPA 2000. This does not apply to other public authorities where internal authorisation is still the norm.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No progress, the scrutiny of new data sharing proposals remains largely similar to previous systems.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A Commission on a Bill of Rights established in March 2011 to recommend a course of action. However the Commission’s final report, in December 2012, showed that they had failed to reach a consensus.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**BIG BROTHER WATCH**

**Pledge:** Defend trial by jury.

**Coalition Policy:**

**Outcome:** No progress.

**Pledge:** Prevent the Collection of Children’s Biometric Data without Permission.

**Coalition Policy:**

**Outcome:** Protection of Freedoms Act 2012 - The verbal consent of the pupil and the written consent of one parent is now required before biometric data is taken by an educational establishment.

**Pledge:** Restore the Right to Protest.

**Coalition Policy:**

**Outcome:** No progress.

**Pledge:** Reform Libel Laws.

**Coalition Policy:**

**Outcome:** Defamation Act 2014 – Higher thresholds for libel cases to be brought and extended protections for publishers. However Northern Ireland is not covered by the legislation.

**Pledge:** Abolish ID Cards and Increase Number of Police Officers.

**Coalition Policy:**

**Outcome:** Identity Documents Act 2010 - Abolished ID Cards and the National Identity Register. Police numbers have been reduced.

**Pledge:** Scrap Plan for Second Generation ePassports.

**Coalition Policy:**

**Outcome:** Coalition Agreement - Plans for the implementation of Second Generation ePassports scrapped, the use of biometric information in passports has been restricted.

**Pledge:** Prevent the Increase in any New Offences.

**Coalition Policy:**

**Outcome:** The proposed ‘stop unit’ hasn’t been established, however there has not been a significant increase in new offences being created.

**Pledge:** Remove Innocent People’s DNA from the Police Database.

**Coalition Policy:**

**Outcome:** Protection of Freedoms Act 2012 – Led to the removal of 1.7m DNA profiles taken from innocent people and children from the NDNAD. However the Scottish DNA model was not established.

**Pledge:** Scrap the ContactPoint Database.

**Coalition Policy:**

**Outcome:** ContactPoint was shut down in August 2010.

**Pledge:** Scrap Control Orders.

**Coalition Policy:**

**Outcome:** Control Orders were replaced with Terrorism Prevention and Investigation Measures (TPIMs), which many critics have argued represent little or no improvement.

**Pledge:** Reduce the length of Pre-Charge Detention.

**Coalition Policy:**

**Outcome:** Protection of Freedoms Act 2012 – Pre-charge detention reduced to 14-days.

---


TPIM – Terrorism Prevention and Investigation Measures, the measure includes electronic tagging, requiring the subject to report to police and ensuring that they must stay in their home overnight. Individuals under a TPIM are also prohibited from travelling abroad and are excluded from entering certain areas.

---

123. See previous section for full figures.

---

See previous section for full figures.

Pledge: Prevent the Collection of Children’s Biometric Data without Permission.  Coalition Policy: Outcome: Protection of Freedoms Act 2012 - The verbal consent of the pupil and the written consent of one parent is now required before biometric data is taken by an educational establishment.


Pledge: Reform Libel Laws.  Coalition Policy: Outcome: Defamation Act 2014 – Higher thresholds for libel cases to be brought and extended protections for publishers. However Northern Ireland is not covered by the legislation.

Pledge: Abolish ID Cards and Increase Number of Police Officers.  Coalition Policy: Outcome: Identity Documents Act 2010 - Abolished ID Cards and the National Identity Register. Police numbers have been reduced.121

Pledge: Scrap Plan for Second Generation ePassports.  Coalition Policy: Outcome: Coalition Agreement - Plans for the implementation of Second Generation ePassports scrapped, the use of biometric information in passports has been restricted.

Pledge: Prevent the Increase in any New Offences.  Coalition Policy: Outcome: The proposed ‘stop unit’ hasn’t been established, however there has not been a significant increase in new offences being created.

Pledge: Prevent Storage of Email and Internet Records.  Coalition Policy: Outcome: The Draft Communications Data Bill was blocked by Nick Clegg in March 2013. Clegg has pledged that the passing of the bill is “certainly not going to happen with Liberal Democrats in government”.122 However, there was widespread support for the Data Retention and Investigatory Powers Act (DRIPA), with only 2 Liberal Democrat MPs voting against it.

Pledge: Remove Innocent People’s DNA from the Police Database.  Coalition Policy: Outcome: Protection of Freedoms Act 2012 – Led to the removal of 1.7m DNA profiles taken from innocent people and children from the NDNAD. However the Scottish DNA model was not established.

Pledge: Scrap the ContactPoint Database.  Coalition Policy: Outcome: ContactPoint was shut down in August 2010.

Pledge: Scrap Control Orders.  Coalition Policy: Outcome: Control Orders were replaced with Terrorism Prevention and Investigation Measures (TPIMs), which many critics have argued represent little or no improvement.123

Pledge: Reduce the length of Pre-Charge Detention.  Coalition Policy: Outcome: Protection of Freedoms Act 2012 – Pre-charge detention reduced to 14-days.

---

121. See previous section for full figures.
123. TPIM – Terrorism Prevention and Investigation Measure, the measure includes electronic tagging, requiring the subject to report to police and ensuring that they must stay in their home overnight. Individuals under a TPIM are also prohibited from travelling abroad and are prohibited from entering certain areas.
THE BIG BROTHER WATCH MANIFESTO

This section highlights the ten key areas that Big Brother Watch believe requires urgent attention in order to protect and enhance our civil liberties. These ten areas are:

1. SURVEILLANCE TRANSPARENCY
2. DATA PROTECTION
3. CCTV AND SURVEILLANCE CAMERA SYSTEMS
4. POWERS OF ENTRY
5. CONTROL OF COUNTER-TERRORISM STRATEGY
6. SOCIAL MEDIA LAW
7. ONLINE CENSORSHIP
8. DIGITAL BILL OF RIGHTS
9. DATA RETENTION AND INVESTIGATORY POWERS
10. INTERCEPT AS EVIDENCE
PART 3
THE BIG BROTHER WATCH MANIFESTO

This section highlights the ten key areas that Big Brother Watch believe require urgent attention in order to protect and enhance our civil liberties. These ten areas are:

1. SURVEILLANCE TRANSPARENCY
2. DATA PROTECTION
3. CCTV AND SURVEILLANCE CAMERA SYSTEMS
4. POWERS OF ENTRY
5. CONTROL OF COUNTER-TERRORISM STRATEGY
6. SOCIAL MEDIA LAW
7. ONLINE CENSORSHIP
8. DIGITAL BILL OF RIGHTS
9. DATA RETENTION AND INVESTIGATORY POWERS
10. INTERCEPT AS EVIDENCE
1. SURVEILLANCE TRANSPARENCY

The UK Government’s response to Edward Snowden’s revelations has been noticeably weak. Big Brother Watch believe that the disclosures regarding the state of the UK’s intelligence network should be seen as an opportunity to initiate much needed and long overdue reforms to the UK’s surveillance system. We acknowledge that the Intelligence and Security Committee’s report into the murder of Fusilier Lee Rigby in Woolwich has enabled some oversight but a great deal more openness and transparency is required.

POLICY RECOMMENDATIONS:

1. A review into the Commissioner system

An effective Commissioner system is vital to ensuring proper oversight of the Intelligence Services. It has become clear that in its current format the system is not fit for purpose. It has been criticised by both the Home Affairs Select Committee (HASC) and Shadow Home Secretary, Yvette Cooper MP, who have called for there to be an ‘overhaul’ in how the system operates. It is vital that there is a thorough review into what improvements can be made. Any review process should focus on three aspects:

- The resources available to each Commissioner must be increased. At present they are insufficient for the task they are expected to accomplish. One clear example is the Intelligence Services Commissioner (InSc) who has a staff of one who functions as his ‘PA’. In the 2011/12 financial year the three main agencies that he is responsible for overseeing had a combined staff of 13,293 and a budget of ‘approximately £2 billion.’ When considering these figures it is understandable why he was only able to examine 12% of the interception warrants authorised in 2011.
- The Commissioners should be full time. Currently these posts are part-time, which curtails the amount of work undertaken.
- The roles should be more public facing. The Commissioners are supposed to ensure that the intelligence and security services are working in the public’s best interests. However, the HASC has raised the important point that many of the public are unaware or confused about their roles. Any review should include recommendations on improving how the Commissioners interact with the public.

2. There should be a full review into necessary reform of the Intelligence and Security Committee (ISC)

As the ISC is the main body tasked with overseeing the work of the intelligence services it is important that it functions effectively and transparently. There are a number of areas that require attention in order to help the Committee fulfil its crucial role. For this reason there must be a full review into how the ISC operates and what improvements are needed in order to make it more effective.

The ISC has made several recommendations for the improvement of the ISC; we fully endorse those proposals, and believe they could be instructive terms of reference for any review. The recommendations include:

- The ISC should become a full parliamentary select committee. This has been recommended by the Home Affairs Select Committee and the Foreign Affairs Select Committee.
- The Committee should be chaired by a member of the Opposition who has had limited prior contact with the intelligence services in their previous posts.
- The Committee should be adequately staffed and resourced. The example of the US system of oversight is particularly instructive here. Whilst the ISC has 9 staff members the US House Permanent Select Committee on Intelligence has 32 members.

We further propose that:

- The Committee’s proceedings should take place in public. There is no reason for the majority of the evidence sessions to be held in secret when successive Directors of the CIA have publically testified to Congress since 1975.
- The Prime Minister should not have the ability to redact a report before it is seen by Parliament.

3. The publication of Government Transparency Reports.

Many technology companies, for example Google, Facebook and Vodafone, now publish sixth monthly or annual transparency reports. These reports provide details of the number of requests for user data that governments have made. This practice began after the US Justice Department reached an agreement with several leading technology companies that allowed them to publish information about the number of Government data requests that they receive. If the UK Government were to follow suit and make its figures publically available, it would greatly increase transparency and better inform the debate around the use of surveillance. This move would have strong public support; a ComRes poll for Big Brother Watch found that 66% of British adults thought the Government should publish more data about how surveillance powers are used.

---

137. Facebook Global Government Requests Report: https://www.facebook.com/about/government_requests
1. SURVEILLANCE TRANSPARENCY

The UK Government’s response to Edward Snowden’s revelations has been noticeably weak. Big Brother Watch believe that the disclosures regarding the state of the UK’s intelligence network should be seen as an opportunity to initiate much needed and long overdue reforms to the UK’s surveillance system. We acknowledge that the Intelligence and Security Committee’s report into the murder of Fusilier Lee Rigby in Woolwich has enabled some oversight but a great deal more openness and transparency is required.

POLICY RECOMMENDATIONS:

1. A review into the Commissioner system

An effective Commissioner system is vital to ensuring proper oversight of the Intelligence Services. It has become clear that in its current format the system is not fit for purpose. It has been criticised by both the Home Affairs Select Committee (HASC) and Shadow Home Secretary, Yvette Cooper MP, who have called for there to be an ‘overhaul’ in how the system operates. It is vital that there is a thorough review into what improvements can be made. Any review process should focus on three aspects124, 125:

- The resources available to each Commissioner must be increased. At present they are insufficient for the task they are expected to accomplish. One clear example is the Intelligence Services Commissioner (InSc) who has a staff of one who functions as his ‘PA.’ In the 2011/12 financial year the three main agencies that he is responsible for overseeing had a combined staff of 13,293 and a budget of ‘approximately £2 billion.’ When considering these figures it is understandable why he was only able to examine 12% of the interception warrants authorised in 2011.126, 127, 128
- The Commissioners should be full time. Currently these posts are part-time, which curtails the amount of work undertaken
- The roles should be more public facing. The Commissioners are supposed to ensure that the intelligence and security services are working in the public’s best interests. However, the HASC has raised the important point that many of the public are unaware or confused about their roles. Any review should include recommendations on improving how the Commissioners interact with the public129

2. There should be a full review into necessary reform of the Intelligence and Security Committee (ISC)

As the ISC is the main body tasked with overseeing the work of the intelligence services it is important that it functions effectively and transparently. There are a number of areas that require attention in order to help the Committee fulfill its crucial role. For this reason there must be a full review into how the ISC operates and what improvements are needed in order to make it more effective.

The ISC has made several recommendations for the improvement of the ISC; we fully endorse those proposals, and believe they could be instructive terms of reference for any review. The recommendations include:130

- The ISC should become a full parliamentary select committee. This has been recommended by the Home Affairs Select Committee and the Foreign Affairs Select Committee131
- The Committee should be chaired by a member of the Opposition who has had limited prior contact with the intelligence services in their previous posts
- The Committee should be adequately staffed and resourced. The example of the US system of oversight is particularly instructive here. Whilst the ISC has 9 staff members the US House Permanent Select Committee on Intelligence has 31

We further propose that:

- The Committee’s proceedings should take place in public. There is no reason for the majority of the evidence sessions to be held in secret when successive Directors of the CIA have publically testified to Congress since 1975
- The Prime Minister should not have the ability to redact a report before it is seen by Parliament

3. The publication of Government Transparency Reports.

Many technology companies, for example Google, Facebook and Vodafone, now publish sixth monthly or annual transparency reports.132, 133 These reports provide details of the number of requests for user data that governments have made. This practice began after the US Justice Department reached an agreement with several leading technology companies that allowed them to publish information about the number of Government data requests that they receive.134 If the UK Government were to follow suit and make its figures publically available, it would greatly increase transparency and better inform the debate around the use of surveillance. This move would have strong public support; a ComRes poll for Big Brother Watch found that 66% of British adults thought the Government should publish more data about how surveillance powers are used.135

129. Ibid p.66
134. Big Brother Watch, Enhancing surveillance transparency: A UK policy framework: http://www.bigbrotherwatch.org.uk/files/briefings/BBW_transparency_2014.pdf 135. ComRes poll 136. Big Brother Watch, a ComRes poll for Big Brother Watch found that 66% of British adults thought the Government should publish more data about how surveillance powers are used.
2. DATA PROTECTION

The public and private sector now have the ability to store some of our most personal information. The legislation that governs the collection and storage of this information is the **Data Protection Act 1998 (DPA)**. In recent years it has become increasingly clear that the Act is not up to the task of deterring the illegal disclosure of our information. Under the legislation the sanctions available to the courts are, in many cases, trivial. When compared to the scale of the losses and the financial rewards which can be gained by selling personal data the current range of punishments is grossly disproportionate.

**POLICY RECOMMENDATIONS:**

1. The introduction of custodial sentences under Section 55 of the Data Protection Act

This is one process which would require minimal effort, but would yield results. Under Section 77 of the **Criminal Justice and Immigration Act 2008** a Secretary of State can implement a custodial sentence of up to 2 years for serious breaches of the DPA.137

No new primary legislation would be required and it would send a clear message that the Government takes the security of personal information seriously. It is a move that has received support from a wide range of bodies including the Home Affairs and Justice Select Committees, the Leveson Report and the Information Commissioner’s Office.

As technology expands further into our everyday lives, devices will be reaching further into our personal and private lives. The grab of granular information, creating big data documents of our health, home and work life, energy use, transport preferences and finances will be greater than ever before. It is critical that effective deterrents for those with access to this highly valuable personal information are established. Privacy and security should be seen as a positive requirement of the future economic wellbeing of the country.

2. The Data Protection Act should be extended to cover information that has been anonymised

The DPA provides little protection for anonymised information. Currently the definition of what is personal data precludes anonymised information from being included. This should be rectified to pre-empt future concerns regarding the creation of large data sets and Big Data projects which will become a greater part of the public and private sector over the coming years. Studies, such as Robust De-anonymisation of Large Sparse Datasets (How to Break Anonymity of the Netflix Prize Dataset), is one of many that show the ease with which it is possible to combine separate databases to re-identify individuals.138


3. CCTV AND SURVEILLANCE CAMERA SYSTEMS

It is estimated that the UK has 20% of the world’s cameras compared to just 1% of the world’s population.139 This reaffirms the need for a strong and robust regulatory system.

As part of the Protections of Freedoms Act 2012 the post of the Surveillance Camera Commissioner (SCC) was created. The Act specified the following duties:

- Encourage compliance with the surveillance camera code
- Review the operation of the code
- Provide advice about the code140

Despite this, the Information Commissioner’s Office (ICO) still oversees the use of CCTV and publishes guidance on its use. It is feared that having multiple points of contact that deal with broadly similar issues can foster confusion. The same can be said for the multiple codes of practice that usually make the same points.

**POLICY RECOMMENDATIONS:**

1. The creation of a single point of contact to resolve CCTV complaints and grievances

In order to give the public clarity over who they can appeal to in order to resolve disputes over CCTV, the ICO’s enforcement powers should be transferred to the SCC. This would reduce confusion over who is responsible for ensuring CCTV is used proportionately and is respectful of the public’s privacy. Another advantage of the SCC being the single point of contact is that it would enable the ICO to concentrate on its other, more diverse responsibilities.

2. The release of a single, enforceable Code of Practice which applies to all CCTV cameras

There should be a single, straightforward Code of Practice that covers all cameras irrespective of their owner. The vast majority of CCTV cameras are operated by private companies and individuals, it has been a failure of successive codes of practice not to recognise this. The Code should also include a range of sanctions to make sure that those who do choose to break it receive appropriate penalties.

139. Daily Mail, UK has 20% of world’s cameras compared to just 1% of the world’s population, 27th March 2007: http://www.dailymail.co.uk/news/article-444819/UK-1-worlds-population-20-CCTV-cameras.html


BIG BROTHER WATCH
2. DATA PROTECTION

The public and private sector now have the ability to store some of our most personal information. The legislation that governs the collection and storage of this information is the Data Protection Act 1998 (DPA). In recent years it has become increasingly clear that the Act is not up to the task of deterring the illegal disclosure of our information. Under the legislation the sanctions available to the courts are, in many cases, trivial. When compared to the scale of the losses and the financial rewards which can be gained by selling personal data the current range of punishments is grossly disproportionate.

POLICY RECOMMENDATIONS:

1. The introduction of custodial sentences under Section 55 of the Data Protection Act

This is one process which would require minimal effort, but would yield results. Under Section 77 of the Criminal Justice and Immigration Act 2008 a Secretary of State can implement a custodial sentence of up to 2 years for serious breaches of the DPA.137

No new primary legislation would be required and it would send a clear message that the Government takes the security of personal information seriously. It is a move that has received support from a wide range of bodies including the Home Affairs and Justice Select Committees, the Leveson Report and the Information Commissioner’s Office.

As technology expands further into our everyday lives, devices will be reaching further into our personal and private lives. The grab of granular information, creating big data documents of our health, home and work life, energy use, transport preferences and finances will be greater than ever before. It is critical that effective deterrents for those with access to this highly valuable personal information are established. Privacy and security should be seen as a positive requirement of the future economic wellbeing of the country.

2. The Data Protection Act should be extended to cover information that has been anonymised

The DPA provides little protection for anonymised information. Currently the definition of what is personal data precludes anonymised information from being included. This should be rectified to pre-empt future concerns regarding the creation of large data sets and Big Data projects which will become a greater part of the public and private sector over the coming years. Studies, such as Robust De-anonymisation of Large Sparse Datasets (How to Break Anonymity of the Netflix Prize Dataset), is one of many that show the ease with which it is possible to combine separate databases to re-identify individuals.138

3. CCTV AND SURVEILLANCE CAMERA SYSTEMS

It is estimated that the UK has 20% of the world’s cameras compared to just 1% of the world’s population.139 This reaffirms the need for a strong and robust regulatory system. As part of the Protections of Freedoms Act 2012 the post of the Surveillance Camera Commissioner (SCC) was created. The Act specified the following duties:

- Encourage compliance with the surveillance camera code
- Review the operation of the code
- Provide advice about the code139

Despite this, the Information Commissioner’s Office (ICO) still oversees the use of CCTV and publishes guidance on its use. It is feared that having multiple points of contact that deal with broadly similar issues can foster confusion. The same can be said for the multiple codes of practice that usually make the same points.

POLICY RECOMMENDATIONS:

1. The creation of a single point of contact to resolve CCTV complaints and grievances

In order to give the public clarity over who they can appeal to in order to resolve disputes over CCTV, the ICO’s enforcement powers should be transferred to the SCC. This would reduce confusion over who is responsible for ensuring CCTV is used proportionately and is respectful of the public’s privacy. Another advantage of the SCC being the single point of contact is that it would enable the ICO to concentrate on its other, more diverse responsibilities.

2. The release of a single, enforceable Code of Practice which applies to all CCTV cameras

There should be a single, straightforward Code of Practice that covers all cameras irrespective of their owner. The vast majority of CCTV cameras are operated by private companies and individuals, it has been a failure of successive codes of practice not to recognise this. The Code should also include a range of sanctions to make sure that those who do choose to break it receive appropriate penalties.

139. Daily Mail, UK has 1% of world’s population but 20% of its CCTV cameras, 27th March 2007: http://www.dailymail.co.uk/news/article-444819/UK-1-worlds-population-20-CCTV-cameras.html
Currently the ability of both local and central government officials to enter private property is far too widespread and the protections available to members of the public are simply not strong enough. Progress on remedying this has been slow and poorly executed. With over 900 ways to enter private property, the legislation is extremely confusing for the average person to understand. Review is required in order to give individuals added protection from unwanted and unnecessary intrusions on their privacy.\(^\text{141}\)

**POLICY RECOMMENDATIONS:**

1. A new review process beginning with a zero-based starting point

Currently many departments don’t know how many powers they have.\(^\text{141}\) A new review process would assess which powers are necessary for local authorities and departments to carry out their functions in an effective manner. The relevant authorities would be able to build up a clear picture of precisely what they need, reducing some of the unnecessary and outdated powers. The outcome would be a more straightforward understanding of what powers of entry exist and when they should be used.

2. The introduction of statutory protection from unnecessary intrusions.

This is an idea first brought forward during the passage of the Protection of Freedoms Act. Any process of this type should require powers to be exercised only with the consent of the owner or by first obtaining a warrant. This would give individuals greater protection from officials illegally entering their homes and workplaces. It would also allow for more judicious and restrained use and go some way towards stopping unnecessary entries.

3. The creation of an enforceable Code of Practice

The current code is unworkable and will be difficult to enforce. It must be rewritten to ensure that powers are used proportionately and not abused. The Code should include clear instructions for what time of day officials can arrive, the number of officers that can be admitted and that in each instance there is a proper explanation of the reasons and the legal basis for an entry.

Any code must include proper sanctions to act as a deterrent to officials wishing to use their powers for trivial or illegal matters.

---

At present the UK’s counter-terrorism strategy is directed by the Metropolitan Police Service (MPS).

An example of the responsibilities in this area include the maintaining of the National Domestic Extremist and Disorder Intelligence Unit database. This gained notoriety when it emerged that Green Party Peer and London Assembly Member, Baroness Jenny Jones, had been recorded on the database in 2001 leading to a dossier of her public and political actions being kept.\(^\text{143}\)

The Home Affairs Select Committee have been critical of these powers being held by the MPS and have proposed that they be transferred to the National Crime Agency (NCA).\(^\text{144}\)

**POLICY RECOMMENDATIONS:**

1. Control of the UK’s counter-terrorism strategy should be given to the National Crime Agency

This is an important step that needs to be taken to ensure the effectiveness of the UK’s law enforcement bodies in combating terrorism. The Home Affairs Select Committee raised the important point that as a national body the NCA has the necessary expertise and authority to oversee these activities.\(^\text{144}\) It would also have the added benefit of allowing the MPS to focus exclusively on policing the capital.

If policy recommendation 1 is carried out, then policy recommendation 2 would be necessary:

2. The National Crime Agency should increase its accountability to the public.

It is vital that the NCA is made subject to the terms of the Freedom of Information Act 2000, making it more transparent and accountable to the public. This is already the case in all other police forces and will help to increase the level of trust within the police and law-enforcement agencies.

---

\(^{141}\) Daily Telegraph, New powers of entry into private homes created by Coalition, 16th March 2012: http://www.telegraph.co.uk/news/politics/9155659/New-powers-of-entry-into-private-homes-created-by-Coalition.html


Currently the ability of both local and central government officials to enter private property is far too widespread and the protections available to members of the public are simply not strong enough. Progress on remedying this has been slow and poorly executed. With over 900 ways to enter private property, the legislation is extremely confusing for the average person to understand. Review is required in order to give individuals added protection from unwanted and unnecessary intrusions on their privacy.\footnote{Daily Telegraph, New powers of entry into private homes created by Coalition, 20th March 2012: http://www.telegraph.co.uk/news/politics/9155659/New-powers-of-entry-into-private-homes-created-by-Coalition.html}

**POLICY RECOMMENDATIONS:**

1. **A new review process beginning with a zero-based starting point**
   Currently many departments don’t know how many powers they have.\footnote{Daily Telegraph, New powers of entry into private homes created by Coalition, 20th March 2012: http://www.telegraph.co.uk/news/politics/9155659/New-powers-of-entry-into-private-homes-created-by-Coalition.html} A new review process would assess which powers are necessary for local authorities and departments to carry out their functions in an effective manner. The relevant authorities would be able to build up a clear picture of precisely what they need, reducing some of the unnecessary and outdated powers. The outcome would be a more straightforward understanding of what powers of entry exist and when they should be used.

2. **The introduction of statutory protection from unnecessary intrusions.**
   This is an idea first brought forward during the passage of the Protection of Freedoms Act. Any process of this type should require powers to be exercised only with the consent of the owner or by first obtaining a warrant. This would give individuals greater protection from officials illegally entering their homes and workplaces. It would also allow for more judicious and restrained use and go some way towards stopping unnecessary entries.

3. **The creation of an enforceable Code of Practice**
   The current code is unworkable and will be difficult to enforce. It must be rewritten to ensure that powers are used proportionately and not abused. The Code should include clear instructions for what time of day officials can arrive, the number of officers that can be admitted and that in each instance there is a proper explanation of the reasons and the legal basis for an entry.
   Any code must include proper sanctions to act as a deterrent to officials wishing to use their powers for trivial or illegal matters.

At present the UK’s counter-terrorism strategy is directed by the Metropolitan Police Service (MPS).

An example of the responsibilities in this area include the maintaining of the National Domestic Extremist and Disorder Intelligence Unit database. This gained notoriety when it emerged that Green Party Peer and London Assembly Member, Baroness Jenny Jones, had been recorded on the database in 2001 leading to a dossier of her public and political actions being kept.\footnote{BBC News, Green Party politician Jenny Jones on ‘domestic extremist’ database, 16th June 2014, http://www.bbc.co.uk/news/uk-england-london-27872451}

The Home Affairs Select Committee have been critical of these powers being held by the MPS and have proposed that they be transferred to the National Crime Agency (NCA).\footnote{Home Affairs Select Committee, Counter-terrorism, Seventeenth Report of Session 2013-14 p.55: http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/231/231.pdf}

**POLICY RECOMMENDATIONS:**

1. **Control of the UK’s counter-terrorism strategy should be given to the National Crime Agency**
   This is an important step that needs to be taken to ensure the effectiveness of the UK’s law enforcement bodies in combating terrorism. The Home Affairs Select Committee raised the important point that as a national body the NCA has the necessary expertise and authority to oversee these activities.\footnote{Ibid, p.55} It would also have the added benefit of allowing the MPS to focus exclusively on policing the capital.

If policy recommendation 1 is carried out, then policy recommendation 2 would be necessary:

2. **The National Crime Agency should increase its accountability to the public.**
   It is vital that the NCA is made subject to the terms of the Freedom of Information Act 2000, making it more transparent and accountable to the public. This is already the case in all other police forces and will help to increase the level of trust within the police and law-enforcement agencies.
6. **SOCIAL MEDIA LAW**

Cases such as the ‘Twitter Joke Trial’, have shown that the current legislation is out of date when it comes to policing social media. The two most widely used laws are Section 127 of the Communications Act 2003 and the Malicious Communications Act 1988. The dates alone highlight the problem of using these pieces of legislation: both were passed before the social media revolution and the launch of Facebook in 2004 and Twitter in 2006.

In response to the growing level of cases that were being brought the former Director of Public Prosecutions, Kier Starmer, introduced a new set of guidelines to inform proceedings which involved social media. The guidelines included:

- The necessity for the communication to be ‘grossly offensive’ or ‘obscene’ for prosecutions to take place
- A definition of ‘grossly offensive’
- The subsequent actions of the interested parties should be considered

**POLICY RECOMMENDATIONS:**

1. **Legislation must be drafted which reflects the changes that have taken place in the communications landscape**

The laws as they stand are out of date and the current guidelines on social media prosecutions, although better than nothing, do not resolve the issue. As a first step Section 127 of the Communications Act should be abolished. The Act itself was first drafted to deal with abuse towards telephone operators and through successive amendments was extended to regulate the one-to-many communications that exist on the internet.

After this section of the Act has been abolished, new legislation applicable to internet communications should be drafted, addressing the specific challenges.

2. **Remove the term ‘grossly offensive’ from the Malicious Communications Act 1988**

Using the term ‘grossly offensive’ is subjective and has resulted in unnecessary and wasteful cases being brought to trial. Loose wording of this kind can have serious implications, there should be real consideration given to the necessity of the phrase.

7. **ONLINE CENSORSHIP**

The Home Office has authorised plans to block extremist websites and content online. Any situation wherein the responsibility for blocking extremist content is left to an unaccountable civil servant who operates within an un-transparent system, should be opposed. Big Brother Watch would encourage a process of judicial oversight to ensure that any decisions made regarding blocking online content has proper legal control and support.

**POLICY RECOMMENDATIONS:**

1. **A clear approach to filtering arrangements**

There has been some confusion over what type of filtering will be utilised in the Government’s strategy. In “Tackling extremism in the UK” the Prime Minister’s Task Force on Tackling Radicalisation and Extremism pledged to “work with internet companies to restrict access to terrorist material online”. However the Home Secretary’s written ministerial statement which accompanied the document made reference to “identifying extremist content to include in family friendly filters”. Amending family filters voluntarily is acceptable and understandable. Blocking content to all customers however would require careful consideration and a clear decision making process.

2. **The implementation of a legally sound blocking process**

Big Brother Watch advocates a system that replicates Section 97A of the Copyright, Design and Patents Act 1988, which requires a High Court injunction to be served on ISPs. A system such as this would be able to fully consider the issues of both criminality and the public interest to freedom of speech.
6. SOCIAL MEDIA LAW

Cases such as the ‘Twitter Joke Trial’, have shown that the current legislation is out of date when it comes to policing social media. The two most widely used laws are Section 127 of the Communications Act 2003 and the Malicious Communications Act 1988. The dates alone highlight the problem of using these pieces of legislation: both were passed before the social media revolution and the launch of Facebook in 2004 and Twitter in 2006.

In response to the growing level of cases that were being brought the former Director of Public Prosecutions, Kier Starmer, introduced a new set of guidelines to inform proceedings which involved social media. The guidelines included:

- The necessity for the communication to be ‘grossly offensive’ or ‘obscene’ for prosecutions to take place
- A definition of ‘grossly offensive’
- The subsequent actions of the interested parties should be considered

POLICY RECOMMENDATIONS:

1. Legislation must be drafted which reflects the changes that have taken place in the communications landscape

The laws as they stand are out of date and the current guidelines on social media prosecutions, although better than nothing, do not resolve the issue. As a first step Section 127 of the Communications Act should be abolished. The Act itself was first drafted to deal with abuse towards telephone operators and through successive amendments was extended to regulate the one-to-many communications that exist on the internet.

After this section of the Act has been abolished, new legislation applicable to internet communications should be drafted, addressing the specific challenges.

2. Remove the term ‘grossly offensive’ from the Malicious Communications Act 1988

Using the term ‘grossly offensive’ is subjective and has resulted in unnecessary and wasteful cases being brought to trial. Loose wording of this kind can have serious implications, there should be real consideration given to the necessity of the phrase.

7. ONLINE CENSORSHIP

The Home Office has authorised plans to block extremist websites and content online. Any situation wherein the responsibility for blocking extremist content is left to an unaccountable civil servant who operates within an un-transparent system, should be opposed. Big Brother Watch would encourage a process of judicial oversight to ensure that any decisions made regarding blocking online content has proper legal control and support.

POLICY RECOMMENDATIONS:

1. A clear approach to filtering arrangements

There has been some confusion over what type of filtering will be utilised in the Government’s strategy. In “Tackling extremism in the UK” the Prime Minister’s Task Force on Tackling Radicalisation and Extremism pledged to “work with internet companies to restrict access to terrorist material online”. However the Home Secretary’s written ministerial statement which accompanied the document made reference to “identifying extremist content to include in family friendly filters”. Amending family filters voluntarily is acceptable and understandable.

Blocking content to all customers however would require careful consideration and a clear decision making process.

2. The implementation of a legally sound blocking process

Big Brother Watch advocates a system that replicates Section 97A of the Copyright, Design and Patents Act 1988, which requires a High Court injunction to be served on ISPs. A system such as this would be able to fully consider the issues of both criminality and the public interest to freedom of speech.
It is clear that the free and neutral nature of the internet is under threat by both government institutions and private companies. If this continues, other countries around the world have threatened policies that would lead to the ‘Balkanisation’ of the Internet wherein countries no longer trust each other so set about carving the web into separate national internets.

**POLICY RECOMMENDATIONS:**

1. **The introduction of a Digital Bill of Rights**

   With June 2015 marking the 800th anniversary of *Magna Carta*, it is time that a similar charter existed to protect our online rights. The document should introduce common standards to safeguard the free and open nature of the internet. This is a concept that has been called for by a variety of figures such as Sir Tim Berners-Lee, Al Gore, Lord Foulkes of Cumnock, Martin Amis and Gillian Slovo.

   151. [Common Dreams, Al Gore: Snowden Revealed ‘Way More Serious’ Than Any He Committed](http://www.commondreams.org/headline/2014/06/10-8)
   152. [Yahoo! News, Peer urges protection from trolls](https://uk.news.yahoo.com/peer-urges-protection-trolls-145452746.html#iU9H5Ss)

**DATA RETENTION AND INVESTIGATORY POWERS**

The Data Retention and Investigatory Powers Bill (DRIP) was published as emergency legislation on the 10th July 2014 and was passed by both Houses on the 17th July 2014 after only 3 days debate. MPs and Peers from all parties criticised the speed at which the Bill went through Parliament, stating that the Government had not allowed enough time for proper scrutiny and damaged public confidence. **Tom Watson MP** stated that “Parliament has been insulted by the cavalier way in which a secret deal has been used... It is democratic banditry, resonant of a rogue state”.

The highly contentious DRIPA contains a sunset clause dated for December 2016. Big Brother Watch welcome the sunset clause and the opportunity for a proper debate on the issues of security and privacy that this will afford.

**POLICY RECOMMENDATIONS:**

1. **The Creation of an independent privacy and civil liberties board**

   During the announcement and debate of DRIPA, the Government stated they would create a privacy and civil liberties oversight board with the American version, Privacy and Civil Liberties Oversight Board (PCLOB), as a template. However, some concerns have been raised regarding the function of the proposed board. **Lord Carlile** has stated “let us be honest about what this board is. It is the counter-terrorism oversight board, and we would do well to adopt the title used in the United States so that it is what it says on the tin”. It is important that the scope of the board is not limited to anti-terrorism issues; it must be allowed to look into all legislation that can invade individuals’ privacy or civil liberties. After all the Home Secretary pushed the passing of DRIPA in order to tackle ‘serious organised crime’ and ‘paedophiles’ as well as terrorists.

   The board should be formed with an appropriately balanced selection of members to ensure proper scrutiny and oversight. As **Baroness Kennedy of The Shaws** stated:

   “The security services are vital to the interests of our nation but they need to be questioned. They need to be questioned with some scepticism at times and I am not sure that we get that when people become comfortable in the security committees... Scrutiny is not of the level that it should be...and I hope we will see on them...some of the people who have been niggling at these issues.”

---

154. [Tom Watson, Commons Hansard Data Retention and Investigatory powers debate](http://www.publications.parliament.uk/pa/cm201415/cmhansrd/cm140715/debtext/140715-0001.htm#14071546000002)
155. [Theresa May, Commons Hansard Data Retention and Investigatory powers debate](http://www.publications.parliament.uk/pa/cm201415/cmhansrd/cm140715/debtext/140715-0001.htm#14071546000002)
156. [Lord Carlile, Lords Hansard Data Retention and Investigatory powers debate](http://www.publications.parliament.uk/pa/cm201415/cmhansrd/cm140715/debtext/140715-0001.htm#14071546000002)
157. [Baroness Kennedy of The Shaws, Lords Hansard Data Retention and Investigatory powers debate](http://www.publications.parliament.uk/pa/cm201415/cmhansrd/cm140715/debtext/140715-0001.htm#14071546000002)
It is clear that the free and neutral nature of the internet is under threat by both government institutions and private companies. If this continues, other countries around the world have threatened policies that would lead to the ‘Balkanisation’ of the Internet wherein countries no longer trust each other so set about carving the web into separate national internets.

POLICY RECOMMENDATIONS:

1. The introduction of a Digital Bill of Rights

With June 2015 marking the 800th anniversary of Magna Carta, it is time that a similar charter existed to protect our online rights. The document should introduce common standards to safeguard the free and open nature of the internet. This is a concept that has been called for by a variety of figures such as Sir Tim Berners-Lee, Al Gore, Lord Foulkes of Cumnock, Martin Amis and Gillian Slovo.


The Data Retention and Investigatory Powers Bill (DRIP) was published as emergency legislation on the 10th July 2014 and was passed by both Houses on the 17th July 2014 after only 3 days debate. MPs and Peers from all parties criticised the speed at which the Bill went through Parliament, stating that the Government had not allowed enough time for proper scrutiny and damaged public confidence. Tom Watson MP stated that “Parliament has been insulted by the cavalier way in which a secret deal has been used… It is democratic banditry, resonant of a rogue state.”

The highly contentious DRIPA contains a sunset clause dated for December 2016. Big Brother Watch welcome the sunset clause and the opportunity for a proper debate on the issues of security and privacy that this will afford.

POLICY RECOMMENDATIONS:

1. The Creation of an independent privacy and civil liberties board

During the announcement and debate of DRIPA, the Government stated they would create a privacy and civil liberties oversight board with the American version, Privacy and Civil Liberties Oversight Board (PCLOB), as a template. However, some concerns have been raised regarding the function of the proposed board.

Lord Carlile has stated “let us be honest about what this board is. It is the counter-terrorism oversight board, and we would do well to adopt the title used in the United States so that it is what it says on the tin”.

It is important that the scope of the board is not limited to anti-terrorism issues; it must be allowed to look into all legislation that can invade individuals’ privacy or civil liberties. After all the Home Secretary pushed the passing of DRIPA in order to tackle ‘serious organised crime’ and ‘paedophiles’ as well as terrorists.

The board should be formed with an appropriately balanced selection of members to ensure proper scrutiny and oversight. As Baroness Kennedy of The Shaws stated: “The security services are vital to the interests of our nation but they need to be questioned. They need to be questioned with some scepticism at times and I am not sure that we get that when people become comfortable in the security committees… Scrutiny is not of the level that it should be…[and] I hope we will see on them…some of the people who have been niggling at these issues.”
Additionally, we believe that in order to have an effective board, the following will also have to be considered:

- The board should be empowered to obtain documents and testimonies that are necessary to its enquiries and empowered to refer misconduct to prosecutors
- There should be a good level of support from technical experts
- There should be transparency and frequent reporting of the Board’s activities

2. Ensure a full system of scrutiny in 2016

During the announcement of the legislation the Deputy Prime Minister, stated that he “only agreed to this emergency legislation because we can use it to kick-start a proper debate about freedom and security in the internet age”. Not only is it important that this debate takes place but it is vital that the debate is conducted properly, with a full discussion and scrutiny of the issues.

We therefore urge the government to ensure the following points are considered:

- There must be a full and thorough consultation with all relevant committees, such as the Home Affairs Select Committee, the Intelligence and Security Committee and the Joint Committee on Human Rights
- All new legislation must be in compliance with the European Court of Justice ruling and laws
- Any concerns stated in the pending 6-monthly reports and other relevant reports must be considered and addressed

10. INTERCEPT AS EVIDENCE

Currently the UK is the only common law country not to allow the use of intercept evidence in court. This was confirmed by a seven year review which concluded it wouldn’t be possible to implement an intercept as evidence model in the UK, stating that it would be too costly to implement such a change.158

The current system makes it very difficult to gather evidence against terror suspects and subsequently have them successfully convicted. Successive governments have seen Control Orders and TPIMs as the solution to this problem when, in fact, the reverse is true. Allowing the use of intercept evidence would be part of the solution to the problem of this repressive legislation.

POLICY RECOMMENDATIONS:

1. Lift the bar on the use of intercept as evidence in court

The idea that the additional costs and an increase in the amount of administrative work should stop a very necessary change in the law is deeply concerning. It is particularly ludicrous considering that every other common law country has managed to implement changes in this area.

By allowing the use of material evidence gathered thorough warranted surveillance, it would be easier to prove the innocence or guilt of suspects and the need to rely on the TPIM regime would be lessened.

Examples from countries which allow the use of intercept as evidence in court show that it is an effective and beneficial tool in the fight against terrorism and serious organised crime.

In the USA intercept evidence was used to charge and convict individuals involved in terror plots within the 48 hour pre-charge detention period. In Australia the former Australian Commonwealth Director of Public Prosecutions, Damian Bugg QC has been quoted as saying:

“The use of telephone intercepts in trials for terrorism offences and other serious crimes is now quite common in Australia and I cannot understand why England has not taken the step as well.”

The Coalition Government in 2010 were supportive of a change in the law on the use of intercept, formerly the Labour Party too have expressed a desire to remove the ban. Big Brother Watch would like to see more specific commitment from all political parties to conduct a transparent and independent review of the law as stands and permit evidence gathered from intercept into court.159, 160


161. Financial Times, Brown backs court use of intercepts, 7th February 2008: http://www.ft.com/content/eb36e96a-0a1f-11dc-9af1-0000779fd2ac


161. Financial Times, Brown backs court use of intercepts, 7th February 2008: http://www.ft.com/content/eb36e96a-0a1f-11dc-9af1-0000779fd2ac

Additionally, we believe that in order to have an effective board, the following will also have to be considered:

- The board should be empowered to obtain documents and testimonies that are necessary to its enquiries and empowered to refer misconduct to prosecutors
- There should be a good level of support from technical experts
- There should be transparency and frequent reporting of the Board’s activities

2. Ensure a full system of scrutiny in 2016

During the announcement of the legislation the Deputy Prime Minister, stated that he “only agreed to this emergency legislation because we can use it to kick-start a proper debate about freedom and security in the internet age”.

Not only is it important that this debate takes place but it is vital that the debate is conducted properly, with a full discussion and scrutiny of the issues.

We therefore urge the government to ensure the following points are considered:

- There must be a full and thorough consultation with all relevant committees, such as the Home Affairs Select Committee, the Intelligence and Security Committee and the Joint Committee on Human Rights
- All new legislation must be in compliance with the European Court of Justice ruling and laws
- Any concerns stated in the pending 6-monthly reports and other relevant reports must be considered and addressed

10. INTERCEPT AS EVIDENCE

Currently the UK is the only common law country not to allow the use of intercept evidence in court. This was confirmed by a seven year review which concluded it wouldn’t be possible to implement an intercept as evidence model in the UK, stating that it would be too costly to implement such a change.139

The current system makes it very difficult to gather evidence against terror suspects and subsequently have them successfully convicted. Successive governments have seen Control Orders and TPIMs as the solution to this problem when, in fact, the reverse is true. Allowing the use of intercept evidence would be part of the solution to the problem of this repressive legislation.

POLICY RECOMMENDATIONS:

1. Lift the bar on the use of intercept as evidence in court

The idea that the additional costs and an increase in the amount of administrative work should stop a very necessary change in the law is deeply concerning. It is particularly ludicrous considering that every other common law country has managed to implement changes in this area.

By allowing the use of material evidence gathered thorough warranted surveillance, it would be easier to prove the innocence or guilt of suspects and the need to rely on the TPIM regime would be lessened.

Examples from countries which allow the use of intercept as evidence in court show that it is an effective and beneficial tool in the fight against terrorism and serious organised crime. In the USA intercept evidence was used to charge and convict individuals involved in terror plots within the 48 hour pre-charge detention period. In Australia the former Australian Commonwealth Director of Public Prosecutions, Damian Bugg QC has been quoted as saying:

“The use of telephone intercepts in trials for terrorism offences and other serious crimes is now quite common in Australia and I cannot understand why England has not taken the step as well.”

The Coalition Government in 2010 were supportive of a change in the law on the use of intercept, formerly the Labour Party too have expressed a desire to remove the ban. Big Brother Watch would like to see more specific commitment from all political parties to conduct a transparent and independent review of the law as stands and permit evidence gathered from intercept into court.160, 161
ABOUT BIG BROTHER WATCH

Big Brother Watch was set up to challenge policies that threaten our privacy, our freedoms and our civil liberties, and to expose the true scale of the surveillance state.

Founded in 2009 by Matthew Elliott, we have produced unique research exposing the erosion of civil liberties in the UK, looking at the dramatic expansion of surveillance powers, the growth of the database state and the misuse of personal information.

We campaign to give individuals more control over their personal data, and hold to account those who fail to respect our privacy, whether private companies, government departments or local authorities.

Protecting individual privacy and defending civil liberties, Big Brother Watch is a campaign group for the digital age.

If you are a journalist and you would like to contact Big Brother Watch, including outside office hours, please call +44 (0) 7505 448925 (24hrs). You can also email press@bigbrotherwatch.org.uk for written enquiries.

WHO WE ARE

RENE SAMSON CHIEF EXECUTIVE

Renate Samson joined Big Brother Watch as Chief Executive in November 2014. She is former Chief of Staff to Rt Hon David Davis MP with whom she worked for five years predominantly on his civil liberties campaigns such as the Snoopers Charter, NHS data sharing, protection for whistleblowers, Reform Section 5 and the DRIP Bill. Prior to working in Parliament, Renate produced documentaries for the BBC, ITV, Sky and other international broadcasters.

EMMA CARR DIRECTOR

Emma joined Big Brother Watch as Deputy Director in February 2012 and was appointed as Director in August 2014. Previously, she worked for political campaign and research groups. Emma has a MSc in Public Services Policy and Management from King’s College London. She has a particular interest in cyber security and cyber crime, which formed the topic of her dissertation.

DANIEL NESBITT RESEARCH DIRECTOR

Daniel joined Big Brother Watch as an intern in December 2012, he quickly became an essential part of the team and was promoted to Researcher in March 2013 and Research Director in August 2014. Before working at Big Brother Watch he interned at Politics Home.

ADVISORY COUNCIL

Heather Brooke
Freedom of information campaigner and Professor of Journalism at City University, London

Rt Hon David Davis MP
Member of Parliament for Haltemprice and Howden

Alex Deane
Managing Director and Head of Public Affairs Strategic Communications at FTI Consulting

Matthew Elliott
Founder of Big Brother Watch, the TaxPayers’ Alliance, Business for Britain, and former Campaign Director of NO2AV

Sir Chris Fox
Former president of the Association of Chief Police Officers

Mark Littlewood
Director General of the Institute of Economic Affairs

Nick Pickles
Twitter UK Public Policy

Henry Porter
Author and journalist

Dominic Raab MP
Member of Parliament for Esher and Walton

Richard Smith
Co-founder of Big Brother Watch

Lord Strasburger
Peer and member of the Joint Committee on the draft Communications Data Bill

Lord Vinson LVO DL
Conservative peer

BIG BROTHER WATCH

CALL: 020 7340 6030
EMAIL: info@bigbrotherwatch.org.uk
POST:
BIG BROTHER WATCH
55 TUFTON STREET, LONDON SW1P 3QL
BIGBROTHERWATCH.ORG.UK
ABOUT BIG BROTHER WATCH

Big Brother Watch was set up to challenge policies that threaten our privacy, our freedoms and our civil liberties, and to expose the true scale of the surveillance state.

Founded in 2009 by Matthew Elliott, we have produced unique research exposing the erosion of civil liberties in the UK, looking at the dramatic expansion of surveillance powers, the growth of the database state and the misuse of personal information.

We campaign to give individuals more control over their personal data, and hold to account those who fail to respect our privacy, whether private companies, government departments or local authorities.

Protecting individual privacy and defending civil liberties, Big Brother Watch is a campaign group for the digital age.

If you are a journalist and you would like to contact Big Brother Watch, including outside office hours, please call +44 (0) 7505 448925 (24hrs). You can also email press@bigbrotherwatch.org.uk for written enquiries.

BIG BROTHER WATCH

CALL: 020 7340 6030
EMAIL: INFO@BIGBROTHERWATCH.ORG.UK
POST: BIG BROTHER WATCH
55 TUFTON STREET, LONDON SW1P 3QL

WHO WE ARE

RENA TE SAMS ON CHIEF EXECUTIVE

Renate Samson joined Big Brother Watch as Chief Executive in November 2014. She is former Chief of Staff to Rt Hon David Davis MP with whom she worked for five years predominantly on his civil liberties campaigns such as the Snoopers Charter, NHS data sharing, protection for whistleblowers, Reform Section 5 and the DRIP Bill. Prior to working in Parliament, Renate produced documentaries for the BBC, ITV, Sky and other international broadcasters.

EMMA CARR DIRECTOR

Emma joined Big Brother Watch as Deputy Director in February 2012 and was appointed as Director in August 2014. Previously, she worked for political campaign and research groups. Emma has a MSc in Public Services Policy and Management from King’s College London. She has a particular interest in cyber security and cyber crime, which formed the topic of her dissertation.

DANIEL NESBITT RESEARCH DIRECTOR

Daniel joined Big Brother Watch as an intern in December 2012, he quickly became an essential part of the team and was promoted to Researcher in March 2013 and Research Director in August 2014. Before working at Big Brother Watch he interned at Politics Home.

ADVISORY COUNCIL

Heather Brooke
Freedom of information campaigner and Professor of Journalism at City University, London
Rt Hon David Davis MP
Member of Parliament for Haltemprice and Howden
Alex Deane
Managing Director and Head of Public Affairs Strategic Communications at FTI Consulting
Matthew Elliott
Founder of Big Brother Watch, the TaxPayers’ Alliance, Business for Britain, and former Campaign Director of NO2AV
Sir Chris Fox
Former president of the Association of Chief Police Officers
Mark Littlewood
Director General of the Institute of Economic Affairs
Nick Pickles
Twitter UK Public Policy
Henry Porter
Author and journalist
Dominic Raab MP
Member of Parliament for Esher and Walton
Richard Smith
Co-founder of Big Brother Watch
Lord Strasburger
Peer and member of the Joint Committee on the draft Communications Data Bill
Lord Vinson LVO DL
Conservative peer
## Our Work In Numbers

<table>
<thead>
<tr>
<th>Category</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>National Press Hits</td>
<td>285</td>
</tr>
<tr>
<td>National Broadcast Hits</td>
<td>67</td>
</tr>
<tr>
<td>Regional Press Hits</td>
<td>837</td>
</tr>
<tr>
<td>International Hits</td>
<td>197</td>
</tr>
<tr>
<td>Total Press Hits Per Year</td>
<td>2073</td>
</tr>
</tbody>
</table>

385,000 People Visited More Than 2.1 Million Times In 2014

20 Consultations Responses

10 Policy Briefings

Big Brother Watch
## OUR WORK IN NUMBERS

<table>
<thead>
<tr>
<th></th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>National Press Hits</td>
<td>285</td>
</tr>
<tr>
<td>National Broadcast Hits</td>
<td>67</td>
</tr>
<tr>
<td>Regional Press Hits</td>
<td>837</td>
</tr>
<tr>
<td>International Hits</td>
<td>197</td>
</tr>
<tr>
<td>Total Press Hits per Year</td>
<td>2073</td>
</tr>
</tbody>
</table>

### More than 2.1 Million Times in 2014

- 385,000 people visited
- 20 consultations responses
- 10 policy briefings

### BIG BROTHER WATCH

- Emma Carr
- BBC News
- 2 AT BBC.co.uk/news
- BBC News
BIG BROTHER WATCH
BIGBROTHERWATCH.ORG.UK

PROTECTING CIVIL LIBERTIES
THE 2015 BIG BROTHER WATCH MANIFESTO