Analysis
UK: New coalition government pledges to "reverse the substantial erosion of civil liberties and roll-back state intrusion"

Max Rowlands

The Conservative-Lib Dem coalition government has made a number of specific commitments to address the considerable damage done by New Labour's 13-year assault on civil liberties. The full-text of the coalition agreement, titled *The Coalition: our programme for government*, pledges, among other things, to scrap identity cards and the National Identity Register (NIR), modify the operational practices of the DNA database, regulate CCTV usage, and review the use of anti-terrorism legislation and data retention.[1]
]
The wording of these commitments is vague and it is uncertain what form they will eventually take. A number of the outgoing government's most unsavoury enactments have also not been adequately addressed. But crucially the new coalition has acknowledged that a problem exists. For this reason civil libertarians have reason to be cautiously optimistic, and the full list of substantive measures makes pleasant reading:

- *We will implement a full programme of measures to reverse the substantial erosion of civil liberties and roll back state intrusion*
- *We will introduce a Freedom Bill.*
- *We will scrap the ID card scheme, the National Identity register and the ContactPoint database, and halt the next generation of biometric passports.*
- *We will outlaw the finger-printing of children at school without parental permission.*
- *We will extend the scope of the Freedom of Information Act to provide greater transparency.*
- *We will adopt the protections of the Scottish model for the DNA database.*
- *We will protect historic freedoms through the defence of trial by jury.*
- *We will restore rights to non-violent protest.*
- *We will review libel laws to protect freedom of speech.*
- *We will introduce safeguards against the misuse of anti-terrorism legislation.*
- *We will further regulate CCTV.*
- *We will end the storage of internet and email records without good reason.*
- *We will introduce a new mechanism to prevent the proliferation of unnecessary new criminal offences.*
- *We will establish a Commission to investigate the creation of a British 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 British law, and protects and extends British liberties. We will seek to promote a better understanding of the true scope of these obligations and liberties.[2]*

Encouragingly, the Conservatives appear to have made concessions by adopting the majority of the proposals the Lib Dems set out in their manifesto and February 2009 draft Freedom Bill. Writing in *The Observer*, Henry Porter suggests that "it is a rare

stroke of luck for the interests of liberty that the coalition allows the prime minister, David Cameron, to embrace this Lib Dem policy with open arms and ignore the reservations of the law-and-order nuts on his right."[3]

This article addresses the most objectionable Labour policies in urgent need of reform. A detailed analysis of all of the measures listed above can be found on the *Statewatch* website.[4]

We will scrap the ID card scheme, the National Identity register and the ContactPoint database, and halt the next generation of biometric passports

It comes as no surprise that identity cards and the National Identity Register (NIR) will be scrapped. Their abolition was a primary manifesto commitment for both the Conservatives and Lib Dems, both of whom had vehemently opposed the *Identity Cards Act 2006*. What is heartening, however, is that the new coalition government has pledged to cancel the introduction of second generation biometric passports even though only the Lib Dems were committed to doing so. Fingerprint records were due to be added to these "e-passports" from 2012.

Passports come under the "Royal Prerogative" and must be amended by an "Order in Council" agreed by the Privy Council (of which cabinet ministers automatically become members) in the name of the head of state, the Monarch. Under this arcane process, the Queen calls a meeting of the Privy Council, usually four or five cabinet ministers, at which they agree the matters before it without discussion. A decision to agree a new law then becomes an "Order in Council" and is subsequently laid before parliament in the form of a listing in the daily order paper. If MPs do not force a negative vote on the floor of the house - a move that is virtually unheard of - it automatically becomes law. Whether an "Order of Council" on second generation biometric passports has been agreed is unknown, and as such there is currently no discernable timescale for the scheme's termination.

The abolition of identity cards and the NIR is more straightforward. They will be scrapped by the *Identity Documents Bill*, which was presented to parliament on 26 May 2010.[5] On 27 May 2010, Theresa May said that identity cards would be abolished within 100 days. The NIR, which has drawn stinging criticism from civil liberty campaigners from its inception, would then be physically destroyed. In many ways publicity surrounding the introduction of identity cards served to mask the creation of the NIR: a massive and unprecedentedly comprehensive database. Labour intended it to hold at least fifty pieces of information on every adult in the UK, including biometric data such as fingerprints, facial images and retina scans. These identifiers would be permanently stored on the database, even after a person's death, and a wide range of government departments and agencies would have access to it.

Essentially, identity cards would simply be an extension of this database that you carry on your person. As would the new biometric passports because, as well as sharing an application process with identity cards, the government intended for passport data to also be stored on the NIR because "it will be far more cost effective and secure."[6] Identity cards, passports and the NIR formed Labour's "National Identity Scheme", the creation of which was readily justified by the need to keep up with other European countries who were adding to the number of biometric identifiers held in their citizens' passports. But while some EU member states are compelled to introduce additional biometrics by the Schengen Acquis, the UK opted-out of this requirement and thus has no legal obligation to follow suit.[7] Perhaps more importantly, no country is obliged to create centralised databases in which to store this data as the UK has done. Germany, for example, has categorically rejected the creation of a national register of fingerprints.

It remains to be seen how quickly and easily ID cards and passports can be disentangled from one another. The UK Identity and Passport Service may not only need a new name, but new legislation to dictate how it functions. At the very least it is likely to need significant restructuring. The new government's comprehensive overhaul of Labour policies in this field will fundamentally alter the way the agency functions and Phil Booth of NO2ID has been quick to warn that this will not be straightforward:

> *Don't imagine for a moment that Whitehall will give up its pet projects, empires or agendas without a fight - battles for which we know it has been preparing for years. Nor should we expect the political, commercial and media proponents of database state initiatives to stand quietly by. The official obsession with identity and information-sharing, the very idea that "personal information is the lifeblood of government" still remains.[8]*

By contrast, the Department for Education has confirmed that the abolition of the ContactPoint (CP) database, another manifesto commitment of both parties, will not require primary legislation.[9] We have been told that the appropriate changes will be made in "due course," but no timetable for this has been established and no indication has yet been given as to what will replace it.

Created under the *Children Act 2004*, and launched in 2009, CP holds personal information on everyone under 18-years of age in England, and is fully operational despite being heavily criticised for routinely invading personal privacy and having insufficient security checks.[10] The database is currently accessible by roughly 390,000 teachers, police officers and social workers and is intended to improve child protection by making it easier for them to work as a team. But there is no way to ensure that the vast number of people with access to CP will utilise sensitive information held on the database appropriately, nor are effective mechanisms in place for identifying misuse. Critics have branded the database "a population-surveillance tool" which does nothing to protect children and argued that it is incompatible with both Article 8 of the European Convention on Human Rights, which guarantees the right to respect for private life, and the UN Convention on the Rights of the Child.[11]

Together, the National Identity Scheme and the CP database would impose cradle to grave surveillance. Manifesto commitments have given the new government not only a clear political mandate to abolish these policies but a moral obligation to do so. If one were needed, an additional motivating factor is to save money: an estimated £86 million was to be spent on identity cards over the next four years, and £134 million on biometric passports.[12]

Significantly, a separate scheme run by the UK Border Agency which requires foreign nationals to apply for a biometric residence permit will continue to issue compulsory identity cards to some successful applicants. The system's legal base is the *UK Borders Act 2007* and it does not use the NIR so will be unaffected by the demise of the National Identity Scheme. The Home Office said it intends to hold the biometric details of 90% of foreign nationals by 2015.[13] *Liberty* has warned of the potentially divisive effect forcing identity cards on specific social groups could have, but the new government has given no indication that it will alter this policy.[14]

We will adopt the protections of the Scottish model for the DNA database

The UK Police National DNA Database is the largest in the world because, since 2004, anyone arrested in England and Wales for any "recordable offence" automatically has a DNA sample taken, regardless of whether charges are ever brought against them – a very low threshold. Any sample taken is then permanently stored in the database. In December 2008, the European Court of Human Rights (ECtHR) ruled that this practice breaches Article 8 of the European Convention on Human Rights which covers the right of respect for private and family life. The UK government responded by introducing a complicated range of clauses in its *Crime and Security Bill* that reduced the length of time the records of innocent people would be held to six years. These changes, which did not adequately comply with the ECtHR's ruling, will not now be introduced.

In opposition, both the Lib Dems and Conservatives had been critical of the operational practices of the database. But while the Lib Dem manifesto is categorical in its assertions that the practice of adding innocent people to the database should be discontinued, and that those without a criminal record should be removed, the wording of the Conservative manifesto is less encouraging. It states: "…we will change the guidance to give people on the database who have been wrongly accused of a *minor crime* an *automatic right* to have their DNA withdrawn"[15] (emphasis added). The implication is that people will still have to request to be removed from the database, and there is leeway for the retention of DNA profiles of those accused - but not charged or convicted - of some crimes.

With the adoption of the Scottish model the Conservatives appear to have held sway on this issue. In Scotland police are not entitled to permanently store the DNA of everyone they arrest, but in specific circumstances, when an individual is accused of a violent or sexual crime, they can retain a sample for three years. Once this period has elapsed the police can then apply to a Sheriff to keep the individual on the database for a further two years. Although certainly less objectionable than the system of data retention currently in place in England and Wales, the Scottish model does not satisfy the Lib Dem commitment to not retain the DNA of innocent people. Campaigning organisations, such as *Genewatch*, have also highlighted the fact that under the Scottish model individuals convicted of minor offences still find themselves on the database for life.[16]

The current database has been criticised for its "function creep", lack of cost-effectiveness and over-representation of ethnic minorities and children. It is unclear if and how the new government will address these issues. They must also contend with a police culture that has become increasingly predicated on arrest-making as a means to acquire peoples' DNA samples.[17] Writing in *The Guardian*, Carole McCartney warned that the reform of legislation governing the DNA database will not be "quick and straightforward" and urged the government to demonstrate that "restoring trust in

the governance of forensic bioinformation is high on its agenda, taking seriously the numerous reports by respected academics on the subject, and engaging properly in open-minded and comprehensive consultation."[18] For now we have been afforded scant detail. Will innocent people currently on the database have to apply to be removed or will this be done automatically? And what of the status of individuals arrested but not convicted of a "serious crime" within the last five years? The importance of these questions is magnified by the Prüm Treaty, incorporated into EU law in June 2007, which gives member states reciprocal access to each other's national databases of DNA profiles, fingerprints and vehicle registrations.

In her first BBC interview as Home Secretary, the only specific commitment Theresa May made regarding the DNA database was to increase its size: "one of the first things we will do is to ensure that all the people who have actually been convicted of a crime and are not present on it are actually on the DNA database."[19] It is to be hoped that this is not where the new government's priorities lie on this issue.

We will further regulate CCTV

This is a Lib Dem manifesto commitment to address the growth of surveillance in public places. Britain is estimated to operate a fifth of the world's CCTV cameras, most of which are owned by private companies whose operational practices and compliance with the *Data Protection Act* are not adequately regulated. Vast sums of public money have also been spent on their introduction. In December 2009, freedom of information requests made by *Big Brother Watch* showed that the number of cameras owned by local councils had almost trebled in less than ten years, from 21,000 to 60,000.[20] But crucially there is no evidence that the use of CCTV cameras helps to prevent or solve crime. In 2008 it was revealed that only 3% of street robberies were solved using CCTV images and the UK has the highest recorded rate of violent crime in Europe.[21]

Technological developments have also meant that the practice is becoming more intrusive. Some cameras are fitted with facial recognition technology to identify suspects, and in the last few years there has been a vast rise in the number of cameras incorporating automatic car number plate recognition software (ANPR). A system to surveil and record the movements of every vehicle on British roads was originally developed by police in March 2006, but has since expanded unchecked. In February 2010, the Association of Police Chief Officers revealed that 10,502 ANPR enabled cameras were passing information to the National ANPR Data Centre. Between 10 and 14 million photographs are being processed every day, many of which contain images of the vehicle's driver and front-seat passengers.[22] These images will be retained for at least two years. Law enforcement agencies in other EU member states can use the database under the Prüm Treaty, and in April 2008 it emerged that the government has also granted access to the USA.[23]

There is also worrying evidence that the ANPR scheme is being dubiously employed. In January 2010, an *Independent on Sunday* report revealed that police are using the technology to meet government performance targets and raise revenue. The report also said that records stored on the ANPR database are "at least 30 per cent inaccurate" leading to wrongful arrests and car seizures.[24] On 4 June 2010, an investigation by *The Guardian* revealed that 150 ANPR cameras, 40 of them "covert", have been installed in predominantly Muslim areas of Birmingham's suburbs to monitor individuals suspected by security agencies of being "extremist."[25] Local councillors and members of the Muslim community were misled over the true nature of the £3 million scheme - they were told it was to tackle vehicle crime, drug-dealing and anti-social behaviour - which was funded by the Terrorism and Allied Matters fund. On 17 June 2010, use of the cameras was temporarily suspended pending a "full and in-depth consultation."

Civil liberty organisations have been consistently critical of the growth of ANPR technology. In April 2010, *Liberty* announced that it intended to launch the first legal challenge to the surveillance system. The organisation's director, Shami Chakrabarti, said:

> *It's bad enough that images and movements of millions of innocent motorists are being stored for years on end…That the police are doing this with no legislative basis shows a contempt for parliament, personal privacy and the law. Yet another bloated database is crying out for legal challenge and we will happily oblige.[26]*

In their Freedom Bill the Lib Dems advocate the establishment of a Royal Commission to make recommendations on the use and regulation of CCTV.[27] For now the new government has simply made an unspecified commitment to introduce new legislation.

We will introduce safeguards against the misuse of anti-terrorism legislation

In their manifestos, the Lib Dems said they would "stop councils from spying on people" and the

Conservatives committed to "curtailing the surveillance powers that allow some councils to use anti-terrorism laws to spy on people making trivial mistakes or minor breaches of the rules." Although neither mentions it by name, both parties are referring to the application of the *Regulation of Investigatory Powers Act 2000* (RIPA). The Act regulates the circumstances and methods by which public bodies can conduct surveillance and investigations, which includes giving them the power to intercept emails and access private communications data. In 2000 only nine organisations could use RIPA powers, but they have subsequently been afforded to nearly 800 public bodies including local councils, the Charity Commission, Ofcom and the Post Office Investigation Branch.

The creation of these powers was justified as a means to combat terrorism and organised crime in exceptional circumstances, but in reality they have been routinely used against members of the public for minor offences. Only the interception of communications data requires a warrant from the Secretary of State; all other powers are currently "self-authorising" which means that a council official can access communications data or authorise a surveillance operation without needing to obtain the approval of an outside authority such as a magistrate or the police.[28]

On 23 May, a *Big Brother Watch* report showed that councils in Great Britain had conducted 8,575 RIPA operations in the past two years at an average of 11 a day.[29] Behaviour that councils have deemed worthy of surveilling includes littering, breaches of planning regulations, letting a dog foul a public footpath, and breaking the smoking ban. In Croydon a council tree officer used RIPA to access the mobile phone records of a builder he believed to have illegally pruned a tree.[30] Astonishingly, councils can authorise weeks of surveillance against individuals suspected of committing these sorts of offences with no obligation to ever inform them that they are being monitored. Statistics published in March 2009 indicated that only 9% of over 10,000 RIPA authorisations led to a successful prosecution, caution or fixed-penalty notice.[31]

The "communities and local government" section of the coalition agreement says:

> *We will ban the use of powers in the Regulation of Investigatory Powers Act (RIPA) by councils, unless they are signed off by a magistrate and required for stopping serious crime.[32]*

While this is certainly an improvement on the existing system the new government should go further and outlaw the practice completely. As Alex Deane, the Director of *Big Brother Watch*, says:

> *Now that the absurd and excessive use of RIPA surveillance has been revealed, these powers have to be taken away from Councils. The Coalition Government plan to force councils to get warrants before snooping on us is good, but doesn't go far enough. If the offence is serious enough to merit covert surveillance, then it should be in the hands of the police.*

The other major piece of anti-terrorism legislation that is being seriously misused is section 44 of the *Terrorism Act 2000*. The act gives police the right to indiscriminately stop and search people without reasonable suspicion in areas that have been designated to be sensitive to national security: this includes the whole of greater London. Police invoked these powers on 256,026 occasions in England and Wales between April 2008 and March 2009. The Metropolitan Police and Transport Police were responsible for 95% of this total. Of this colossal figure only 1,452 stops resulted in arrest, less than 0.6% of the total number, and the vast majority of these were for offences unrelated to terrorism.[33] In June 2010, the Home Office revealed that, since 2001, procedural errors in 40 separate section 44 police operations have led to thousands of people being unlawfully stopped and searched.[34] Most of these operations were illegal because they had lasted beyond the 28 day statutory limit, and some had not been authorised by the Home Secretary as is required by law.

Section 44 powers have been used to intimidate protestors and impede photography in public places. A climate of suspicion has been cultivated in which anyone taking a photograph of a prominent building or landmark is potentially seen to be conducting reconnaissance ahead of a terrorist attack. Worse still, some police officers believe photography in section 44 areas to be illegal and there is a mountain of anecdotal evidence of photographers, both professional and amateur, being obstructed in public spaces.[35]

In January 2010, the ECtHR found section 44 to breach Article 8 of the European Convention on Human Rights which provides the right to respect for private life. [36] The judgment objected not only to the manner in which anti-terrorism powers are being used, but the whole process by which they are authorised. Parliament and the courts are not providing sufficient checks and balances against misuse and police officers are afforded too much individual autonomy when deciding whether to stop and search someone. The Labour government

appealed against this decision with little chance of success, and on 30 June 2010 the ECtHR ruled that its judgment in the case was final. On 8 July 2010, Theresa May announced that the police would no longer be able to use section 44 powers against individuals, only vehicles. Instead they will now need to use section 43 of the *Terrorism Act* which can be invoked anywhere in the country but crucially requires the police to demonstrate reasonable suspicion that a person is involved in terrorist activity before stopping and searching them. [37]

This is a welcome development, but amending police practice and ensuring that section 43 powers do not come to be routinely misused in much the same way section 44 powers have been will be no easy task. In the last two years the National Policing Improvement Agency, the Home Office and even the Prime Minister had all published guidance to the police on the use of section 44 powers reaffirming the rights of photographers with negligible result. [38]

We will end the storage of internet and email records without good reason

Announced in October 2008, the Interception Modernisation Programme (IMP) is a Labour initiative to intercept and record every phone call, text message, email, chat-room discussion and website visit made in the UK. The content of what was said or written would not be retained, but email and website addresses, phone numbers and contact information from social networking services including instant messengers, Facebook and Skype would be held. The government initially planned to store this data in a massive central database, but by April 2009 had decided it would be more practical to outsource this responsibility to Communications Service Providers (CSPs): primarily internet service providers and telecommunications companies.

Since 2003, these organisations have already retained subscriber and traffic data as part of a "voluntary code" under the *Anti-Terrorism, Crime and Security Act 2001*. The Labour government believed that the practice should be made mandatory and, facing heavy opposition in the UK from the House of Lords, sought an agreement at EU level which would carry the force of European law. It used its rotating presidency of the EU Council to "railroad" the *EC Data Retention Directive 2006* through the legislative process using a mix of political pressure and moral imperative following the 7 July 2005 terrorist attacks on London. The Directive compels member states to store citizens' telecommunications data for a period of six to 24 months but, significantly, does not provide safeguards over who can access this data and on what grounds. In 2007, the "voluntary code" for CSPs was made mandatory by statutory order (meaning no debate) with the justification that the UK was merely fulfilling its obligations under EU law.[39]

The IMP would oblige CSPs to increase drastically the volume of information they hold on their customers for access by police and security services. Under the *Regulation of Investigatory Powers Act 2000*, these bodies can currently access retained data simply on the basis of an "authorisation" by a senior officer, with no form of judicial scrutiny. This led UK law enforcement agencies to access personal communications records a staggering 1.7 million times (1,164 times per day) between 2005 and 2009, in what surely included speculative 'fishing', data-mining and subject-based profiling exercises.[40] All data stored under the IMP could be accessed in exactly the same way.

Responding to an April 2009 government consultation document, *Protecting the Public in a Changing Communications Environment*, many CSPs expressed grave concern over the cost and technical feasibility of intercepting data on such a grand scale.[*41]* As a result of these misgivings, and fearful of negative publicity in the run-up to the May 2010 election, the government dropped a bill to establish the scheme from the November 2009 Queen's speech. However, in the same month, information provided in a written parliamentary answer by a Home Office minister revealed that this would not delay the creation of the IMP which the government expected to be fully operational by 2016.[42]

The Lib Dems have been consistently critical of the IMP and promised in their manifesto to "end plans to store your email and internet records without good cause." In October 2008, Chris Huhne argued that "the government's Orwellian plans for a vast database of our private communications are deeply worrying" and that "these proposals are incompatible with a free country and a free people."[43] The Conservatives have also been critical of the IMP, but promised only to review the scheme and made no mention of it in their manifesto. In January 2010, then shadow security minister, Baroness Pauline Neville-Jones, said that the Labour government had not provided "any evidence to suggest that the universal collection, retention and processing of communications data would actually provide more value to intelligence and law enforcement investigations than the targeted collection of communications data in relation to specific individuals or groups."[44]

Whatever policy it eventually adopts, the problem facing the new government is that the UK is legally

bound to implement the EU Data Retention Directive: it cannot opt out. This means that while access to retained data can be better restricted, for example by requiring judicial authorisation before data can be accessed, and the length of time records are held can be reduced to six months, fundamentally the new government is currently unable to abandon Labour's data retention regime, whether it desires to or not.

Footnotes

1. The Coalition: our programme for government, p. 11: http://www.cabinetoffice.gov.uk/media/409088/pfg_coalition.pdf
2. The Coalition: our programme for government, p. 11: http://www.cabinetoffice.gov.uk/media/409088/pfg_coalition.pdf
3. The Guardian, 16.5.10: http://www.guardian.co.uk/commentisfree/2010/may/16/henry-porter-civil-liberties-coalition
4. A Statewatch full analysis of every proposed measure can be found at: http://www.statewatch.org/analyses/no-104-coalition-government-civil-liberties.pdf
5. See: http://www.number10.gov.uk/queens-speech/2010/05/queens-speech-identity-documents-bill-50641
6. Commons Hansard written answers text, 6 April 2010: http://www.publications.parliament.uk/pa/cm200910/cmhansrd/cm100406/text/100406w0029.htm#column_1269W
7.See Statewatch analysis: UK and Irish opt-outs from EU Justice and Home Affairs (JHA) law, June 2009: http://www.statewatch.org/news/2009/jun/uk-ireland-analysis-no-4-lisbon-opt-outs.pdf
8. Email message to supporters, 14.5.10
9. Kable website, 26.5.10: http://www.kable.co.uk/contactpoint-scrapping-dfe-education-lacks-date-26may10
10. For example see: The Guardian, 22.6.07: http://www.guardian.co.uk/society/2007/jun/22/childrensservices.comment
11. The Guardian, 28.2.07: http://www.guardian.co.uk/commentisfree/2007/feb/28/comment.children
12. The Times, 28.5.10: http://www.timesonline.co.uk/tol/news/politics/article7138094.ece
13. The Independent, 26.9.08: http://www.independent.co.uk/news/uk/home-news/first-sight-of-the-id-cards-that-will-soon-be-compulsory-942802.html
14. Liberty press release, 27.5.10: http://www.liberty-human-rights.org.uk/news-and-events/1-press-releases/2010/27-05-10-id-cards-to-be-scrapped-but-must-be-scrapped-for-all.shtml
15. Conservative Manifesto 2010, p 80: http://media.conservatives.s3.amazonaws.com/manifesto/cpmanifesto2010_lowres.pdf
16. See: http://www.genewatch.org/sub-539489
17. See: Statewatch volume 19 no. 4
18. The Guardian, 20.5.10: http://www.guardian.co.uk/politics/2010/may/20/law-dna-fingerprint-evidence-reform
19. BBC website, 12.5.10: http://news.bbc.co.uk/1/hi/uk_politics/election_2010/8678271.stm
20. Big Brother Watch website, 18.12.09: http://www.bigbrotherwatch.org.uk/home/2009/12/big-brother-is-watching-local-council-controlled-cctv-cameras-treble-in-a-decade.html
21. The Guardian, 6.5.08: http://www.guardian.co.uk/uk/2008/may/06/ukcrime1
22. Kable website, 3.2.10: http://www.kable.co.uk/national-anpr-data-centre-police-acpo-03feb10
23. The Telegraph, 21.4.08: http://www.telegraph.co.uk/news/uknews/1896241/New-anti-terrorism-rules-allow-US-to-spy-on-British-motorists.html
24. The Independent on Sunday, 17.1.10: http://www.independent.co.uk/news/uk/crime/the-laughing-policemen-inaccurate-data-boosts-arrest-rate-1870416.html
25. The Guardian, 4.6.10: http://www.guardian.co.uk/uk/2010/jun/04/birmingham-surveillance-cameras-muslim-community
26. The Times, 4.4.10: http://www.timesonline.co.uk/tol/news/uk/crime/article7086783.ece
27. The Freedom Bill, part 2 chapter 4 explanatory note: http://freedom.libdems.org.uk/the-freedom-bill/7-regulation-of-cctv
28. The police are using RIPA on a grand scale to trawl through vast quantities of personal communications data, as is detailed later in this article.
29. Big Brother Watch website 23.5.10: http://www.bigbrotherwatch.org.uk/home/2010/05/the-grim-ripa-local-councils-authorising-11-covert-surveillance-operations-a-day.html
30. This is Croydon Today website, 3.11.09: http://www.thisiscroydontoday.co.uk/news/Council-uses-anti-

terror-laws-pruned-tree/article-1466974-detail/article.html
31. BBC website, 26.3.09: http://news.bbc.co.uk/1/hi/7964411.stm
32. The Coalition: our programme for government, p. 12:
http://www.cabinetoffice.gov.uk/media/409088/pfg_coalition.pdf
33. Home Office Statistical Bulletin 2008/09: http://www.homeoffice.gov.uk/rds/pdfs09/hosb1809.pdf
34. The Guardian, 10.6.10: http://www.guardian.co.uk/uk/2010/jun/10/anti-terror-law-illegal-stop-search
35. See: Statewatch volume 18 no 3 and volume 19 no 4
36. Case of Gillan and Quinton v. The United Kingdom (Application no. 4158/05), 12.1.10: http://www.statewatch.org/news/2010/jan/echr-judgment-gillan-quinton.pdf
37. The Guardian, 8.7.10: http://www.guardian.co.uk/law/2010/jul/08/anti-terror-stop-and-search-scrapped
38. Amateur Photographer website, 5.12.09:
http://www.amateurphotographer.co.uk/news/Photographers_campaign_forces_police_Uturn_AP_comment_news_292612.html
39. See: http://www.opsi.gov.uk/si/si2007/uksi_20072199_en_1
40. So far four sets of figures have been put on record: 1 January 2005 - 31 March 2006: 439,054; 1 April - 31 December 2006: 253,557; 2007: 519,260; 2008: 504,073: http://www.statewatch.org/uk-tel-tap-reports.htm
41. The Register website, 9.11.09: http://www.theregister.co.uk/2009/11/09/imp_hold; Protecting the Public in a Changing Environment, April 2009:
http://www.official-documents.gov.uk/document/cm75/7586/7586.pdf
42. Kable website, 17.11.09: http://www.kable.co.uk/communications-interception-programme-continues-17nov09
43. BBC website, 15.10.08: http://news.bbc.co.uk/1/hi/uk_politics/7671046.stm
44. Silicon.com website, 22.1.10: http://m.silicon.com/management/public-sector/2010/01/22/which-of-labours-big-it-projects-will-survive-the-tory-axe-39501472/10/