A Free Country?

Damian Green MP

A lecture to the Centre for Policy Studies

15 July 2009

Introduction

There are many aspects of modern British politics which should disturb any thoughtful lover of democracy. Healthy scepticism about the motives and actions of the powerful has switched into unhealthy cynicism about the whole Parliamentary system and those who are required to operate within it. To recover some semblance of respect, we politicians need to show not only that we can clean up our own act, but actually use the democratic process to change the country and lives of everyone in it.

We need to start with that basic right, freedom. It sounds apocalyptic, but I believe it is true, to say that some of the underlying freedoms which underpin Parliamentary democracy are being seriously eroded. What is even more dangerous is that they are being eroded from the best of motives, by well-meaning people who would be hurt and horrified to be regarded as anti-democratic; many of them the most senior officials in this country, holding positions of great trust. Permanent Secretaries and police chiefs can be much more dangerous to British democracy than demagogues and extremist politicians, because they make the rules and define the terms of acceptable debate. If you challenge them you are, almost by definition in Britain, a crank and an outsider, not quite fit to be taken seriously.

A few weeks ago David Cameron spoke about Control State Britain and the surveillance society that we have become. A David Cameron Government would tackle one of the dangers inherent in an over-centralised over-powerful state by devolving power away from Whitehall. As he put it in the Guardian in May "I believe in the central objective of the new policies we need should be a massive, sweeping radical redistribution of power; from the state to citizens; from the government to parliament; from Whitehall to communities; from the EU to Britain; from judges to the people; from bureaucracy to democracy.

This is the kind of redistribution of power that will be the starting point for a Conservative Government; transferring power and control directly to individuals."

A free country?

I want today to illuminate one corner of this noble endeavour. I believe that we have unthinkingly put the interests and convenience of state institutions above those of the citizen. The reason we have done this is not because our rulers are evil. It is much more subtle than that, and therefore more dangerous. It is because the civil service and the security services take it as an article of faith that what they seek to do is in the interests of the wider public. Therefore, the easier it is for them to perform their particular functions the better the public is served. I reject this basic proposition. I believe Government can do harm even when it is seeking to do good. The role of that currently derided figure, the democratically elected politician, is not just to maintain a sceptical attitude to the power of the state, but to organise the state's affairs so that the citizen has some personal space in which the state has no power, interest, or influence.

This aim fits perfectly with the aspiration of David Cameron's I have already quoted. The ultimate aim is to enable individuals to take as much control over their own lives as possible. One the biggest threats to this is an all-encompassing state; a controlling state. Ostensibly good intentions from the state to provide more security, better public services and secure personal identity are significant attacks on our privacy, liberty and choice.

There are currently three streams of state control which flow together to form a river which is toxic to our basic freedoms. These are:

- A national security approach which puts policing needs above all others
- The transformational government agenda
- The "Identity Management" programme.

So far I have been talking in pretty abstract terms. I will come down to earth by listing the databases set up by Government as a result of one or more of these three basic policy frameworks. There are 28 of them:

- National Identity Register
- E-borders
- National DNA Database
- Police National Computer
- National Fingerprint Database
- ASSET - youth offender profiling database
- UKvisas Biometrics Programme
- National Offender Management System

- Automatic Number Plate Recognition
- Communications Database which could monitor all online traffic
- NHS Detailed Care Record
- NHS Summary Care Record
- NHS Secondary Uses Service
- NHS Population Demographics Service
- ContactPoint, a database collecting sensitive information on every child
- ONSET, a Home Office database predicting which children will offend in the future
- National Pupil Database, all children in state education, including nurseries
- National Childhood Obesity Database
- PAYE – Pay As You Earn tax collection system (Treasury)
- Tax Credits Database
- Child benefits Database
- Common Assessment Framework – children's welfare needs
- DWP Customer Information System, described as 'one of the largest databases in Europe'
- DWP Tell Us Once (data-sharing between departments)
- Analytical Data Integration for Government (anonymised data from across government departments)
- Child Maintenance and Enforcement Commission (CSA)
- National Fraud Initiative
- Driving Standards Agency

I invite everyone hearing or reading this to play the party game of working out on how many of these databases your private details feature.

A policing-led state

The first of the three streams, and in many ways the most difficult to challenge, is the security aspect. We live in a dangerous world. There are evil people fired up by powerful ideologies who want to kill us indiscriminately, and don't care how many of their supporters they kill in the process. The security services including the police need resources and support to fight them.

However the approach this Government has taken rests on two questionable assumptions. The first is that we should regard this as a war in the traditional sense—indeed it has been called the War on Terror. Life during wartime is different. Individual needs are downgraded, indeed in some cases eliminated, in the interest of the wider community. Terrorism is not going to go away during the coming years, so we appear to have moved to living in wartime conditions perhaps for the rest of our lives. There is no public assent to this Orwellian state of affairs. If our individual security is to be sacrificed for national security then the terrorists have already won a significant victory over liberal democracy. We must not hand them that victory.

The International Commission of Jurists recently warned that the UK, amongst other countries, is "'creating a dangerous situation wherein terrorism, and the fear of terrorism, are undermining basic principles of international human rights law.' The report claimed many measures introduced were illegal and counter-productive.

There are a number of examples of this, of which the use of stop and search is the most clear.

Lord Carlile, the Independent Reviewer of Terrorism, said in his June 2009 report:

> "Examples of poor or unnecessary use of *section 44*[stop and search for terrorism purposes] abound. I have evidence of cases where the person stopped is so obviously far from any known terrorism profile that, realistically, there is not the slightest possibility of him being a terrorist, and no other feature to justify the stop.
>
> I believe that it is totally wrong for any person to be stopped in order to produce a racial balance of the section 44 statistics. There is ample anecdotal evidence that this is happening.
>
> I am sure that safely it could be used far less. There is little or no evidence that the use of section 44 has the potential to prevent an act of terrorism as compared with other statutory powers of stop and search. While arrests for other crimes have followed searches under the section, none of the many thousands of searches has ever resulted in a conviction of a terrorism offence."

The second questionable assumption is that the most effective way to fight terrorism is to make all of us suspects. Information on everyone in this country needs to be collected,

stored and shared because a few people are planning evil acts. From a narrow policing perspective this might make sense. But the second order effects are disastrous. National Security is best served if the whole country is on the side of the security services. Increasingly, this is not the case. The battle of Law and Order versus Crime should be us and them. If we are all on the police computer systems then the signal is sent to all of us that we are Them.

As David Cameron has said "It's the reason so many innocent citizens mistrust and even fear the police—the very people who should be protecting them—and why so many people increasingly feel that the state is their enemy, not their ally."

I am not making the accusation that we live in a police state—that would be ridiculous. The problem is that we are living in a policing-led state. Police needs are driving policy in this area with no sense of balance between the legitimate demands of the police and the need to preserve the freedom and privacy of the citizen. The irony, of course, is that allowing the police to lead the agenda makes their job more difficult in the long run. Everyone wants "policing by consent" as the ideal for an effective British-style policing model. The police are in danger of losing that consent.

Examples of the policies that illustrate this are legion. Identity Cards are held up as a way of increasing our security, even though Charles Clarke admitted they would not, for example, have prevented the London bombings on July 7th 2005. The DNA database contains the records of nearly one million innocent people, including me. How many of those million are just that bit less likely to want to help the police ever again?

There is a serious related problem, which is that to prevent crime the police want information on the innocent, on the off-chance that they will one day commit a crime. It is bad enough when the police behave like this, as for example in Brighton when they will be visiting a thousand addresses before the Labour Party conference to check the identity of those living there, before cross-checking all of them with the police national computer.

Even worse, this intrusive pre-emptive policing method is now spreading to other authorities, with the same harmful effect on public confidence.

Let's look at the misuse of RIPA: the Regulation of Investigatory Powers Act.

- Burnley borough council. Senior officials authorised surveillance under RIPA to monitor one of their own officials who they suspected of using the gym in office hours

- Hambleton District Council in Yorkshire. Routinely uses RIPA laws to spy on dog walkers using covert video cameras to spy on dog fouling. The snooping is justified since "the dog warden is unable to be in attendance 24 hours a day, 7 days a week".

Some of these people may have been committing minor offences. But the use of what were meant as powers to be used against serious criminals and terrorists helps destroy confidence in public bodies. If we are all suspects, then none of us will help the authorities. That way lies the atomisation of society.

A technology-led state

The second stream flowing into the river of stifling control is the snappily titled "Transformational Government—Enabled by Technology", launched in 2005. This is a programme which has understandably not grabbed the tabloid headlines since it was launched, but it should command serious attention, because in practice it signals the end of privacy for any British citizen. The three original aims were that:

- Services enabled by information technology must be designed around the citizen and business
- There must be an increased culture of shared services to release efficiencies
- There must be a broadening and deepening of government's information technology and professionalism.

The first of these is largely cosmetic, and the third largely comic, given the various project disasters that have hit the state sector in recent years. But the second is key, and highly sinister. It has its roots in a false analogy with the private sector, which has indeed used ICT to provide services more efficiently and cheaply. The difference of course, is that in almost all industries any private sector operator cannot compel us to use its services. Government can not only compel us to use them, but can change the rules, and the terms and conditions, whenever it suits.

In the end, a private sector operator that misuses its customers' data faces the collapse of its business. After criticism of its privacy policies, Facebook was forced to hold a vote amongst its customers on the level of security they expected it to attach to their personal data. This resulted in it having to retreat from previous policies enabling highly targeted advertising on its site.

Successful sites from Amazon to last.fm openly use previous data provided by users, but they have a voluntary relationship. This is not the case with the users of the CSA or the passport service. The analogy used by the advocates of Transformational Government simply does not hold.

The practical result of this is that the ever-increasing number of public-sector databases are being geared up to share information with each other. The cost of running Britain's state-run databases over the next ten years has soared to £34 billion. This is presented as being for the convenience of the citizen, when the overwhelming driver is the convenience of the state. Even the technological solution proposed is old-fashioned and centralist. Government still tends to set up one big computer system to address a single

issue, such as health records. A modern Government, as George Osborne has pointed out, would set up an open source system which does not dictate the technology adopted by users from the centre. This is cheaper and more efficient. Of course it makes keeping personal data private easier, because it does away with the need for a central server. It is therefore not surprising that moves towards open source government has not attracted the British government.

Quite apart from the technical problems of the current system, look at the cost. The UK public sector spends over £16 billion a year on IT. Over £100 billion in spending is planned for the next five years, and even the Government cannot provide an accurate figure for the cost of its 'Transformational Government' programme. Yet only about 30% of government IT projects succeed

Whose identity is it?

The third stream comes under the general heading "identity management". This term covers the complete reversal of the previous understanding of the relationship between the consumer and business, and the citizen and the state. The onus is now on the individual to retain and protect his "identity", instead of the responsibility of those who whom he interacts to know he is who he says he says. A decade ago, banks had a problem with fraud. Now, if someone steals your account details, you have a problem with "identity management." Even worse, if a Government department loses your details, it is a problem for you not the state.

All this means that you need to sign up to compulsory systems which will be backed by biometric information, fingerprints or eye scans, just to prove who you are. The National Identity Register will require almost 50 pieces of personal information, including biometrics such as fingerprints, a picture of your face, and possibly the scanning of your eyeballs.

The Holy Grail for enthusiasts of this policy direction is a "Single Source of Truth" by which the state can know who the citizen is and what he does. The Single Source of Truth is not a phrase made up by paranoid anarchist-inclined civil libertarians, it is the phrase used throughout official papers on this subject. I do not need to rehearse the numerous failings of Government data security systems in recent years to point out the dangers of this ambition. I cannot believe many British people want their Government to hold the Single Source of Truth about them.

If the system fails, the consequences are disastrous. As the comedian Frankie Boyle has put it, before now if someone stole your credit cards you had to make a phone call to cancel them and get new ones. In the future you will need to change your eyeballs. We will have moved from Orwell to Kafka, and perhaps beyond.

What is to be done?

In the words of someone who would have loved the National Identity Register, Lenin, what is to be done?

I would suggest five principles to determine the relationship of the citizen and the state, and three tests which should be applied to technological developments in the delivery of public services. The five principles are:

- The citizen must have control over his own identity
- The whole population must not be treated as potential suspects
- The delivery of public services should not be determined by technology alone
- Policing needs should be only one of the competing needs in a free society
- The risk of failure in a Government system should not be borne by the citizen

The three tests for policy proposals in this area are control, choice, and consent. Applying these tests will enable the principles to be met across all three of the problem areas I have identified.

To be specific, under the heading control the citizen should be able to hold his own identity information. This is perfectly possible, as shown by security freeze laws passed in 47 US states. This allows the citizen to control his personal data through the right to freeze, or lock access, to their credit file against anyone trying to open up a new account or to get new credit in their name. This has been so effective that several private companies operating in states without the law are voluntarily offering their customers the right to freeze their data. 35 states have also given citizens the right to be notified when a government agency loses their confidential information.

Every audit trail of information should be known to the citizen, and only the citizen should decide who has access to the audit trail. Only a properly warranted security officer with a specific purpose should be able to intrude in an unwanted fashion on this audit trail. National security and personal security are both legitimate aims of public policy, and the balance between them needs to be redressed.

The law must in some cases dictate the transaction between the citizen and state: whether we pay taxes or are entitled to a particular benefit. But apart from these transactions the test of choice would mean that the basic choice, of whether to engage or not in a particular transaction with the state, would be the citizen's. In transactions such as the claiming of benefits, when clearly an identity needs to be proved, it will be for the citizen to assert his identity in a suitable way. It may be slightly inconvenient to have to take a passport or driving licence to show your picture to an official, but if the alternative is to give up the choice of whether you can prove who you are, this seems hugely preferable. The world, and our privacy, will be safer if there are multiple sources of truth.

The test of consent would ensure that you have explicitly approved of what is being done with your private information. The notion of "implied consent" (such as is being used in NHS databases) which means that unless you explicitly withdraw from a system it is assumed that you agree to your information being available to all is a dangerous nonsense. Private companies have to make you agree explicitly to them using your information. It is if anything more important that the state should have to go through similar hurdles before using it. Google or the Nectar card companies may know lots about you, but at least they can't arrest you on the basis of what you may have told them. If something goes wrong, then there must be a powerful system of redress, perhaps in the form of greatly enhanced powers for the Information Commissioner.

Conclusion

At present, we are turning into a society where increasingly we are dependent on the goodwill of the state to live our daily lives. In an era when technology gives us citizens more information and therefore power as compared to big private and public institutions, this is not just undesirable, it is completely unnecessary. Whatever the motives of those within Government who aspire to control the Single Source of Truth about every one of us, they must be stopped. From Muslims who resent being regarded as potential terrorists, to parents concerned about their child's schooling, the database capacity of the state has been misused in a way that alienates the otherwise respectable from authority.

There are a number of practical steps we can implement:

We could scrap unnecessary schemes such as the National Identity Register and ID Cards and the Contact Point for children.

We could reform the use of some of the most intrusive databases; such as removing the innocent from the DNA database (I should declare an interest at this point), and reforming the E-Borders scheme so that it does not hold information about the completely innocent for 10 years,

We can end the dominance of suppliers which have led to the plethora of big Government IT schemes. Instead we should be more creative and open-minded about how we procure and provide pubic sector technology, looking to localist and individualist solutions. No more Big Government Computer Schemes, which these days are precisely the wrong approach.

Above all we must change our mindset. Just because technology has transformed way Government can use personal information does not mean that a sensible government will take that choice. In all eras of technology, the principle that the state should serve the citizen and not vice versa is a good one. The bigger the capacity to collect and share information, the greater danger there is to privacy, and therefore to freedom. It is time for the freedom fighters of the world to fight back against the controlling state.