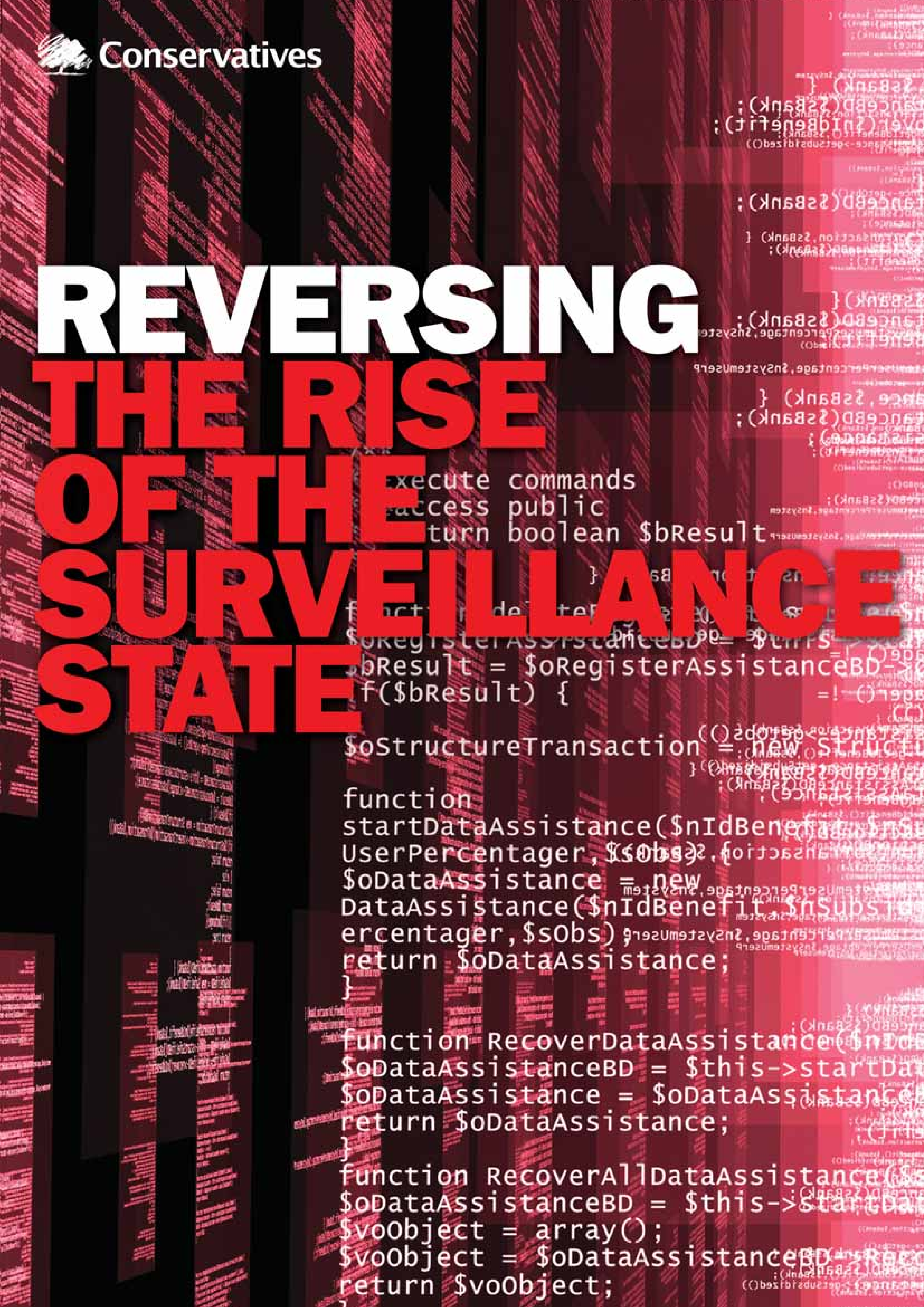
Conservatives

REVERSING THE RISE OF THE SURVEILLANCE STATE



```
execute commands
access public
turn boolean $bResult

bResult = $oRegisterAssistanceBD->
f($bResult) {

$oStructureTransaction = new Struct

function
startDataAssistance($nIdBenefit,$nS
UserPercentager,$sObs) {
$oDataAssistance = new
DataAssistance($nIdBenefit,$nSubsi
ercentager,$sObs);
return $oDataAssistance;
}

function RecoverDataAssistance($nId
$oDataAssistanceBD = $this->startDa
$oDataAssistance = $oDataAssistance
return $oDataAssistance;
}
function RecoverAllDataAssistance(
$oDataAssistanceBD = $this->startDa
$voObject = array();
$voObject = $oDataAssistanceBD->Rec
return $voObject;
```

REVERSING THE RISE OF THE SURVEILLANCE STATE

11 Measures to Protect Personal Privacy and Hold Government to Account

Dominic Grieve QC MP, Shadow Justice Secretary
Eleanor Laing MP, Shadow Justice Minister
September 2009

EXECUTIVE SUMMARY

New Labour has excessively relied on mammoth databases and wide powers of data-sharing, on the pretext that it will make government more effective and the citizen more secure. Its track record demonstrates the opposite, with intrusive and expensive databases gathering masses of our personal information - but handled so recklessly that we are exposed to greater risk.

A Conservative government will take a fundamentally different approach. We believe that your personal information belongs to you, not the state. Where private details are collected by government, they are held on trust. The government must be held accountable to its citizens, not the other way round. We would be guided by the following principles:

- Fewer – not more – giant central government databases.
- Fewer personal details, accurately recorded and held only by specific authorities - on a need-to-know basis only, and for limited periods of time.
- Wherever possible, personal data will be controlled by individual citizens, who have the power to decide which agencies can access or modify this information.
- Greater checks on data-sharing between government departments, quangos and local councils.
- Stronger duties on government to keep the private information it gathers safe.

In practice, this means:

- Scrapping the National Identity Register and ContactPoint database.
- Establishing clear principles for the use and retention of DNA on the National DNA Database, including ending the permanent or prolonged retention of innocent people's DNA.
- Restricting and restraining local council access to personal communications data.
- Reviewing protection of personal privacy from the surveillance state as part of a British Bill of Rights.
- Strengthening the audit powers and independence of the Information Commissioner.
- Requiring Privacy Impact Assessments on any proposals for new legislation or other measures that involve data collection or sharing at the earliest opportunity. Require government to consult the Information Commissioner on the PIA and publish his findings.
- Immediately submitting the Home Office's plans for the retention of - and access to - communications data to the Information Commissioner for pre-legislative scrutiny.
- Requiring new powers of data-sharing to be introduced into law by primary legislation, not by order.
- Appointing a Minister and senior civil servant (at Director General level) in each government ministry with responsibility for departmental operational data security.

- Tasking the Information Commissioner to publish guidelines on best practice in data security in the public sector.

- Tasking the Information Commissioner to carry out a consultation with the private sector, with a view to establishing guidance on data security, including examining the viability of introducing an industry-wide kite mark system of best practice.

INTRODUCTION

'Knowledge without integrity is dangerous and dreadful.'

Samuel Johnson[1]

In 2004 the Information Commissioner, Richard Thomas warned that the creeping intrusions of the state were turning Britain into a 'surveillance society'.[2] Two years on, he gave the following bleak assessment:

> *'Today I fear we are in fact waking up to a surveillance society … As ever-more information is collected, shared and used, it intrudes into our private space and leads to decisions which directly influence people's lives. Mistakes can also easily be made with serious consequences – false matches and other cases of mistaken identity, inaccurate facts or inferences, suspicions taken as reality, and breaches of security. I am keen to start a debate about where the lines should be drawn. What is acceptable and what is not?'*[3]

Five years on, the government has ignored Richard Thomas's original warning. It has compiled a series of unwieldy databases. It is in the process of introducing identity cards, with fifty items of personal information on everyone living in Britain held on a central register. The Home Office has proposed a new Communications Data Bill, to retain – and share across Whitehall - details of every private phone call made, e-mail sent (or received) and access to the internet.

The government recently tried to introduce unprecedented powers, in the Coroners and Justice Bill, which would have allowed the Home Secretary to expand data-sharing between government departments, public bodies, local authorities and even companies by order – without adequate scrutiny or safeguards. The move was successfully resisted by the Conservatives and other opposition parties.

The growth of government databases has been inspired by New Labour's view of the relationship between the state and the citizen, which allows central and local authorities wide powers of command and control over our lives.

This trend is also attributable to New Labour's failure to recognise the technological changes that are changing corporate structures and approaches to information. New technologies are enabling information to be dispersed, and held locally rather than in centralised databases or mainframes. This approach is not only less expensive than constructing a giant central database, but it is also more secure and enables individuals to exercise greater personal control over their data.

Gordon Brown has personally driven government strategy, as Chancellor and Prime Minister. Sir David Varney, one of his closest advisers, was appointed to reform public services through a process of 'transformational government'. Sir David's initial report urged government departments to focus on the 'totality of the relationship with the citizen', 'identity management' and creating 'a single source of truth' on the citizen.[4] The report called for the coordination and pooling of personal data to achieve cost savings. It claimed that the risks would largely be shielded from view, because:

> 'The public do not see this process. They experience only public services packaged for their needs.'[5]

This model was based on the untested presumption that the state has an unfettered right to intrude into the private life of its citizen, both to make them more secure and to facilitate delivery of public services.

The rise of New Labour's database state has been compounded by the expansion of other surveillance powers. The result has been a seismic shift in the relationship between the citizen and the state, at the expense of the former. In 2007, Privacy International (an NGO that monitors privacy issues around the world) ranked Britain's privacy protections joint 43rd out of 47 countries surveyed – with the worst record in Europe, and only marginally better than Russia and China.[6] The report described Britain as an 'endemic surveillance society'.

Contrary to New Labour's assumptions, the public are now all too aware of the growing risks. An ICM poll in 2008 found that 53% of people were not confident that government, councils and banks would protect their personal information. 77% worried more about the safety of their personal details than they used to, with 72% saying they felt powerless to protect such data.[7]

In reality, the approach adopted by Ministers has proved woefully naive of the potential risks and liabilities involved in large government-run database projects. The trade-off between personal privacy and security has proved a mirage. As Sir Ken McDonald, former Director of Public Prosecutions, commented in his valedictory speech in 2008:

> 'We need to take very great care not to fall into a way of life in which freedom's back is broken by the relentless pressure of a security state.'[8]

THE VULNERABILITIES OF NEW LABOUR’S DATABASES

This Government has a long track record of losing the personal data entrusted to it, whilst failing to secure and properly manage its databases. Far from making us more secure, Labour’s databases have exposed us to greater risks. Some of the more serious recent episodes over the last three years include:

- **Criminal Records Bureau (CRB):** In May 2006, the Home Office admitted that 2,700 people were wrongly labelled criminals as a result of checks conducted through the Criminal Records Bureau since its launch in 2002. In response the Home Office statement said: “We make no apology for erring on the side of caution. This is not about the CRB making mistakes.” (Home Office cited in *Times,* 22 May 2006).

- **Information on Failed Asylum Seekers:** Former Home Secretary, John Reid, admitted in July 2006 that as many as 450,000 failed asylum seekers are resident in the UK. He said that Borders and Immigration Agency has a “case-load of around 400,000 to 450,000 electronic and paper records which ….are riddled with duplication and errors”. (Hansard, 19 July 2006, Column 324) It was reported that the filing system in the immigration department “sometimes consists of cardboard files on a windowsill covered in Post-It Notes” (*BBC news online*, 19 July 06).

- **Overseas Convictions Scandal:** In January 2007 it emerged that hundreds of criminals convicted of serious crimes abroad could have been cleared to work with vulnerable people after a failure by the Home Office to enter their details onto the Police National Computer. Information on convictions in 27,500 cases was left “sitting in desk files” in the Home Office rather than being properly examined. (ACPO evidence to Home Affairs Committee, 9 January 2007). It subsequently emerged that these case files contained details of 540 serious offenders including killers, rapists, paedophiles, attempted murderers and drug traffickers (*Hansard*, 10 Jan 2007, Column 286).

- **Court data loss:** In February 2008 a laptop computer holding information on hundreds of convicted criminals was stolen from a Birmingham Magistrates' Court. The theft from the Victoria Law Courts in Birmingham was reported on January 14, West Midlands Police confirmed. The laptop was stolen from an office at the court over the Christmas period, according to Her Majesty's Courts Service (HMCS) (*Birmingham Post*, 8 February 2008).

- **Junior doctors data:** In April 2007, it emerged that the personal details of hundreds of junior doctors were available online after a security error at the body responsible for recruitment. Addresses, telephone numbers, sexual orientation, religion and even previous convictions could be seen on any computer after an error at the NHS Medical Training Application Service website. Those accessing the website could merely tap on a foundation course applicant's name and scroll across to reveal the private details. (*Times,* 26 April 2007).

- **Her Majesty’s Customs and Revenue (HMRC):** In November 2007, Chancellor, Alastair Darling was forced to admit that the personal records of 25 million individuals, including their dates of birth, addresses, bank accounts and national insurance numbers had been lost by HMRC. Paul Gray, chairman of HM Revenue & Customs, resigned after it was confirmed that two computer disks containing the authority's entire data relating to child benefit payments - records for 7.25 million families - had been lost in the post. (*Hansard,* 20 Nov 2007, Column 1101). It later emerged that six further discs containing confidential recorded conversations between a member of staff and a customer making a complaint were lost in transit between the tax credit office in Preston and HMRC's Whitehall headquarters in London. In 2007 alone, there were 2,110 other reported breaches of security at HMRC (Hansard, 29 October 2007, Column 905W).

- **18,000 personal records from the Department of Work and Pensions (DWP):** In December 2007, it was revealed that 18,000 personal records were found at a former DWP contractor's home. The contractor still had unencrypted compact discs containing the details of thousands of benefit claimants, despite having stopped working for the DWP a year before. The two discs held up to 9,000 names each (*BBC Online*, 1 December 2007).

- **DVLA data:** In December 2007 Transport Secretary, Ruth Kelly, was forced to admit that the personal details of more than three million learner drivers had gone missing. The names, addresses and telephone numbers for every candidate who applied for a driving theory test between September 2004 and April 2007 were on a computer hard drive which was lost in May at a supposedly secure facility in the US. (Hansard, 17 Dec 2007, Column 624)

- **MOD data:** In January 2008, it emerged that a laptop computer containing the details of 600,000 people was stolen from the MOD. The laptop listed the personal information of recruits to the Royal Navy, Royal Marines and Royal Air Force, and of others who had expressed an interest in joining. It contained passport details, national insurance numbers, drivers' licence information, family details, doctors' addresses and NHS numbers. The Ministry of Defence said the laptop was stolen from a Royal Navy officer's car parked in Birmingham on 9 January but it had decided - after consulting the police - not to disclose the theft immediately. Defence Secretary, Des Browne, later admitted the loss of two further laptops containing more sensitive information (*Hansard,* 21 Jan 2008, Column 1225)

- **MoD admits 658 laptops stolen**: Defence Secretary Des Browne was forced to re-issue and revise upwards previous estimates of the number of laptops stolen from 347 to 658 in the last four years after 'anomalies in the reporting process' were discovered. In addition the MoD said that 89 laptops had been lost. The department also said that 26 portable memory sticks containing classified information had been either stolen or misplaced since January. In a separate response, ministers said that 131 of the department's USB memory sticks had been taken or misplaced since 2004 (*The Telegraph*, 19 July 2008).

- **National DNA database:** Under Labour, the National DNA database has grown to five million samples, the largest in the world per head of population. The costs of service delivery have doubled since 2002, when the rules were changed to allow permanent retention of innocent people's DNA (*National DNA Database Annual Report 2006/7*). Yet, total detected crimes in which a DNA match was available have dropped by 16.5 per cent between 2002-03 and 2007-08 (*Hansard*, 4 February 2009, Column 1244WA). There are thought to be a million innocent people on the database and yet there are over two million people with a police record without a profile on the DNA database (Hansard, 5 November 2008, Column 602WA). In 2008, the European Court of Human Rights held that the government's arbitrary approach breached the right to privacy (*S. and Marper v. United Kingdom*, 4 December 2008). The Government has long ignored calls from the Conservatives for a Parliamentary debate on the database and for it to be put on a proper statutory footing. In May 2009, and despite the *Marper* ruling, it announced that innocent people's DNA would still be retained for a maximum period of 12 years.

The risk to the public has been compounded by the cavalier attitude of Ministers. Amidst rising concerns, Gordon Brown brushed aside recent data losses, conceding:

> '*We can't promise that every single item of information will always be safe*.'[9]

Yet neither this belated acknowledgment of the government's poor track record, nor the impact on public confidence, has inhibited the scale of its database ambitions. If anything, we face worse to come.

The government is in the process of a phased **introduction of ID cards**, which will store fifty items of personal information on each individual on a central database.

One by one, each grandiose claim for ID cards has crumbled. First, it was claimed that ID cards would tackle benefit fraud. Yet, the overwhelming majority of benefit fraud involves people lying about their personal circumstances – with a fraction of cases involving misrepresentation of identity.[10] Furthermore, the technology is itself vulnerable to cloning and fraud.

Next, Ministers claimed that ID cards would prevent illegal immigration. However, there is an exemption from ID cards for all short-term visitors coming to the UK for under three months. Even if that loophole was closed, research shows that the IT used in both biometric passports and ID cards can easily be cloned.[11]

At various points, Ministers have tried to claim that ID cards would help prevent terrorism. However, the vast majority of terrorists do not hide their identity, actively seeking notoriety. Spanish ID cards did not stop the Madrid bombers in 2004, Turkish ID cards did not stop the Istanbul bombers in 2003 and German ID cards did not stop the Hamburg terrorist cell that planned 9/11. In Britain, ID cards will do little to stop British-based bombers since it will not be mandatory to carry and produce the card on request. Nor could ID cards protect Britain from foreign terrorists - because short stay visitors will not be required to hold one. As the Home Office's former Security Minister was forced to concede:

> *'Perhaps in the past the Government, in its enthusiasm, oversold the advantages of identity cards. We did suggest, or at least implied, that they may well be a panacea for identity fraud, for benefit fraud, terrorism, entitlement and access to public services.'*[12]

Besides their ineffectiveness, privacy campaign groups, like Liberty and NO2ID, warn that the ID cards will also intrude into our privacy. The proposed scheme would enable government departments and companies to share masses of our personal data – including name, date of birth, addresses, identity records, photographs, signature and fingerprints – allowing the state to continuously track the movements and transactions of every citizen.[13] The Information Commissioner Richard Thomas expressed 'increasing alarm' that ID cards are:

> *'… beginning to represent a very significant sea change in the relationship between the state and every individual in this country.'*[14]

Whilst the government has sought to give assurances about privacy protection, safeguards and limits, the ID cards legislation gives the Home Secretary wide powers to extend the scope and remit of the ID cards regime by order, adding a further risk of mission creep once the system is fully operational. Far from making us more secure, Microsoft's National Technology Officer, Jerry Fishenden, warned that the national identity register will create a 'honey pot effect'- attracting hackers, fraudsters and potentially terrorists to try to hack into the register.[15] According to Fishenden, this could trigger 'massive identity fraud on a scale beyond anything we have seen before.'

In May 2008, the government announced further plans for a **Communications Data Bill** based on an EU Directive. It was later reported that proposals were being developed to allow every telephone, email, internet and mobile phone record in Britain to be stored on a single government-run database, accessible to a range of public bodies.[16] The government is currently reviewing its plans for this legislation in response to widespread concerns.

In 2009, the government introduced further proposals in the Coroners and Justice Bill to enable **data-sharing to be expanded by order** of the Secretary of State – without adequate Parliamentary scrutiny - facilitating data-sharing between government, public bodies, local authorities, foreign governments and businesses. The measure was eventually withdrawn after pressure from the Conservatives and other opposition parties, and amidst concern that private medical records could be passed on without patient consent.[17]

In January 2009, it emerged that Ministers estimated that 390,000 officials and other authorised users would be given access to **ContactPoint**, the national government database containing details of 11 million children. The move was widely criticised as increasing the scope for abuse of vulnerable children.[18]

In March 2009, a wide-ranging report by the Joseph Rowntree Reform Trust found that **a quarter of public-sector databases are 'almost certainly illegal'**, fewer than 15% are effective and secure, co-author Professor Ross Anderson describing Britain's database state as a 'financial, ethical and administrative disaster'.[19]

In February, even former Home Secretary David Blunkett spoke out against plans for wider data-sharing and monitoring of communications, warning that the government is leading Britain towards a 'Big Brother' state, and cautioning that: 'If we tolerate the intolerable, the intolerable gradually becomes the norm'.[20]

PROTECTING PERSONAL PRIVACY IN THE TWENTY-FIRST CENTURY

A Conservative government will take a fundamentally different approach. Our starting point is that personal information belongs to the citizen, not the state. Where private information is collected by government, quangos or local authorities, it must be held on trust. In turn, the government must be held accountable to the citizen, rather than the other way around. A Conservative approach will be guided by the following, basic, principles:

- We want to see fewer - not more – giant centralised databases, amassing personal information on the citizen.
- Government should be guided by the principle of proportionality, which means that fewer personal details are accurately recorded and held by specific authorities on a need-to-know basis only, and for limited periods of time justified on the basis of operational necessity.
- Wherever possible, personal data will be controlled by individual citizens, who have the power to decide which agencies can access or modify this information.
- We need greater checks on data-sharing between government departments, quangos and local councils.
- We need stronger duties and sanctions on government, to ensure that the private information it gathers is held securely and that government databases are properly managed.

In practice, the Conservatives propose eleven measures to protect personal privacy and hold government to account:

Fewer Databases, Greater Protection of Personal Privacy

> *1. Scrap the National Identity Register and ContactPoint databases, flawed systems that will create greater – not less – public exposure to risk.*

A Conservative government will deploy IT and databases when it can be done securely, without exposing the public to greater risks. The National Identity Register and Contact Point are costly systems, which are seriously flawed and expose the public to unnecessary risk and the taxpayer to unacceptable contingent liabilities. The resources absorbed could be better deployed towards other practical measures within their relevant departmental programs. As such, a Conservative government would scrap both databases and deploy the resources to more effective measures.

> *2. End the permanent retention of innocent people's DNA on the National Police DNA database.*

The Conservative Party support the use of DNA in a proportionate manner to detect crimes and prosecute offenders. However, the indefinite retention of DNA on the database of people who have never been convicted of a crime is unacceptable in a society founded on the basis that someone is innocent until proven guilty. Following the recent judgment of the European Court of Human Rights in *S. and Marper v. United Kingdom*, 4 December 2008, the Government is required to review the permanent retention of the DNA of those arrested but not convicted of a criminal offence. In May, the Home Secretary announced that – despite the *Marper* ruling - innocent people's DNA would still be retained for up to 12 years.

The Conservatives have taken the lead by announcing the principles that a Conservative Government would apply to the retention of DNA. These include:

- DNA should be retained only whilst a person remains subject to investigation or until criminal proceedings have concluded and should only be used for the purposes of investigating and detecting crime.

- The DNA of adults convicted of a recordable offence should be retained indefinitely.

- No DNA samples or profiles should be retained from adults not convicted of a crime. A limited exception should be made for those charged with certain crimes of violence and serious sexual offences. In these cases, DNA on the National DNA Database or the Counter-Terrorism DNA Database may be retained for a period of 3 years, which could be extended to a maximum of 5 years, if approved by a Crown Court Judge.

- No DNA samples or profiles should be retained on children under the age of 10 (the age of criminal responsibility).

- When a child under the age of 18 is convicted of serious violence or a serious sexual offence, DNA should be retained indefinitely. In the case of conviction for any other recordable offences DNA should only be retained for a period of 5 years.

- The operation of DNA Databases should be subject to independent oversight.

3. Restrict and restrain council access to personal communications data

The bugging and monitoring of phones, emails and internet access has increased dramatically since Labour's Regulation of Investigative Powers Act 2000 (RIPA). The use of intrusive surveillance powers has not been confined to police and intelligence agencies investigating terrorism and other serious crime.

By 2008, there were over 1,000 interception operations initiated under RIPA every day in Britain, and over 600 public bodies entitled to monitor intercepted communications data – over three quarters of which are local councils.[21]

Over three-quarters of those bodies granted these powers are not using them, suggesting both that they are being provided when they are not strictly necessary, and that they are excessively relied upon by a relatively small proportion of public bodies. Publicly available information is limited. However, the annual reports from the Prime Minister to Parliament reveal that this expansion has led to a regular and increasing misuse of the powers available – with 1,088 errors made in the exercise of interception powers in 2006 rising to 1,182 in 2007.

The Conservatives recognise the challenge our police forces and intelligence services face in keeping track of terrorists and those engaged in serious crime. However, the creeping use of intrusive surveillance powers by local authorities represents a disproportionate intrusion into the personal privacy of local residents, without having demonstrated any countervailing law enforcement justification.

A Conservative government will restrict and restrain the exercise of any such powers by local councils. First, RIPA will be amended so that councils will only be allowed access to communications data for the purposes of assisting investigation into serious crimes (those subject to a custodial sentence). Second, any request to access communications data will require the approval of the Council leader, thereby ensuring a measure of democratic accountability. Third, council access to such communications data will require the prior approval of a warrant by the magistrates courts, providing a judicial safeguard.

4. Reviewing protection of personal privacy from the surveillance state as part of a British Bill of Rights.

The Conservative party has pledged to replace the Human Rights Act with a British Bill of Rights. As part of our ongoing review in this area, we will be examining the current level of protection of the individual against the surveillance state, with a view to strengthening personal privacy in a Bill of Rights.

Strengthening the Independence and Powers of the Information Commissioner

5. Strengthen the audit powers and independence of the Information Commissioner.

The Information Commissioner has proved one of the bulwarks against the rise of the surveillance state, providing early warnings and technical advice on the growing concerns over data security. However, the current role is limited and could be strengthened to ensure the Information Commissioner has the necessary independence and powers to hold government to account. In due course, we will also be examining the Information Commissioner's role in overseeing the Freedom of Information system, in light of our commitment to radical reform to achieve far greater transparency in public sector spending and wider governance.

At this stage, we propose that the following reforms:

- The Information Commissioner will be appointed by Parliament rather than the Ministry of Justice.

If the Information Commissioner is to be an effective guardian of the public interest against privacy intrusions by government, he cannot be appointed by government.

We will consult on the detail of the appointment process and organisational structure, based on the operational experience of analogous models including the Electoral Commission, Parliamentary Ombudsman and other bodies.

- The Information Commissioner will be required to audit government departments and other pubic bodies, on a rotating annual basis, and granted the powers required to discharge these functions. These will include ad hoc powers of inspection and financial penalties for the deliberate, reckless or grossly negligent management of data.

In order to improve standards of data security, and inhibit the introduction of unwieldy and unmanageable data systems, Ministers, government departments and officials must be properly held to account. We believe that rather than burdening the public sector with onerous new regulation and red-tape, a more effective means would be to ensure greater audit and sanctions for the worst abuses of data security.

Pursuant to the proposals advanced by the Conservatives during the course of the Coroners and Justice Bill 2009, the Information Commissioner's investigative powers would be increased to allow for ad hoc inspections. That will ensure the Information Commissioner can make an accurate assessment of data security practices, including after any serious breaches.

Furthermore, the power to issue financial penalties to government departments or other public bodies enacted as sections 55(A) to (E) of the Data Protection Act, pursuant to amendments proposed by the Conservatives under the Criminal Justice and Immigration Bill 2008, must be immediately brought into force. This will give 'teeth' to the enhanced role of the Information Commissioner and penalise reckless data security practices, without disproportionately disrupting the work of government departments. A Conservative government will bring these much needed powers into force as a matter of priority.

The Information Commissioner will be given statutory reporting responsibilities for auditing the data security practices of government departments and public bodies, on a rotating basis, to ensure maximum transparency and accountability. This will shift the focus of Ministerial minds onto the implementation of appropriate operational standards of data security, and away from creating novel hair-brained schemes that are a recipe for disaster.

- The Information Commissioner will be required to report directly and annually to Parliament on the discharge of all of these functions

In line with the requirement for the Information Commissioner to be appointed by Parliament - and further to its enhanced powers of investigation, audit and sanction - he will report directly to Parliament on an annual basis on the discharge of all of these functions.[22]

Greater Scrutiny of Data Legislation

> *6. Require Privacy Impact Assessments of any proposals for new legislation or other measures that involve data collection or sharing at the earliest opportunity. Require government to consult the Information Commissioner on the PIA and publish his findings.*

In other civil and common law jurisdictions, including France and New Zealand, the legal regulatory framework requires government departments to consult with their respective information watchdogs, before the development of any scheme for the collection and sharing of data. [23]

This allows the proportionality of such proposals to be considered and the principles of data minimization built into any plans for the scheme at an early stage. Concerns can be aired and practical recommendations built into the design of the scheme at the outset.

A key problem in the United Kingdom in recent years has been that databases have been built and then issues of data security have been addressed as 'bolt on' considerations rather than considered as integral to the initial design. PIAs have not been produced for the NHS Spine, the National Identity Register, Contactpoint, the National DNA database or the Communications Database. Ministers recently confirmed that departments are not under any obligation to produce PIAs.[24]

The Home Affairs Select Committee report 'A Surveillance Society?', published on 8 June 2008, recommended in the context of the Home Office that '[t]he effectiveness of information-sharing should be assessed at the stage at which a new project is proposed, in order to prevent unnecessary sharing and retention of data'[25]. In its reply, the government failed to commit to such early scrutiny or the introduction of Privacy Impact Assessments (PIA) at the earliest stage of preparation of new policies or legislation.[26]

A Conservative government would adopt both proposals, not just for Home Office projects, but for all major public sector programs designed to increase data-collection, sharing or retention. We will make it compulsory for all government departments to undertake a PIA, before developing a new data collection scheme or undertaking a data sharing project with another government department, public body or other third party.[27]

Such a PIA system will ensure that government departments properly consider the impact of any data collection or sharing scheme on individual privacy, and will require them to consider the proportionality of the scheme at the outset.

We would futher require that the Information Commissioner be consulted on the PIA, with his findings and recommendations appended to the PIA on publication.

> *7. Immediately submitting the Home Office's plans for the retention of - and access to - communications data to the Information Commissioner for pre-legislative scrutiny.*

In line with the above recommendations, current Home Office plans for a Communications Data Bill to require the retention, and sharing across Whitehall, of communications data – including details of every private phone call made, e-mail sent (or received) and access to the internet - should be immediately subject to a Privacy Impact Assessment. The Home Office should conduct the PIA in consultation with the Information Commissioner, and the outcome of the review published and reported to Parliament.

> *8. Require any new powers of data-sharing to be introduced into law by primary legislation, not by order, so that they are properly debated and scrutinised in Parliament.*

In 2009, the government introduced further proposals through the Coroners and Justice Bill to enable data-sharing to be expanded by order of the Secretary of State – without adequate Parliamentary scrutiny (see above). The measure was withdrawn in March, following pressure from the Conservatives and other opposition parties, and amidst widespread public concern, including that private medical records could be passed on without patient consent.[28]

Expanding the powers of the surveillance state through secondary legislation vests excessive power with Ministers, and constrains the scope for effective Parliamentary debate and scrutiny. A Conservative government would amend the Data Protection Act 1998 to ensure that any future scheme or proposals extending powers of data collection, sharing or retention must be enacted by primary legislation, to ensure maximum transparency and debate.

Greater Government Responsibility

> *9. Appoint a Minister and senior civil servant (at Director General level) with responsibility for operational data security.*

The new regime proposed will promote higher operational standards of data security. In order to strengthen compliance with best practice, we propose that a Minister assume responsibility for data security in each department. Day-to-day operational matters could be delegated to a senior civil servant, at the level of Director General, with appropriate levels of qualification (based on industry best practice) and experience in data protection, but with the Minister retaining ultimate responsibility. This will create the organisational structure and leadership to drive higher standards of data security.

In the case of the child benefit records lost by HMRC in 2007, Ministers insisted that proper procedures were in place, and attributed the security breaches to the failures of a junior civil servant. This abdication of Ministerial responsibility avoids accountability for data security and demoralises the civil service.

The new structure proposed would create clearer lines of accountability to be followed at the very top of government departments. It will require senior management to monitor data security at every level of their organisation - and take responsibility for consequences rather than just procedures.

> *10. Task the Information Commissioner to publish guidelines on best practice in data security in the public sector.*

We would promote a relationship of dialogue, as well as accountability, between government departments and the Information Commissioner. The Information Commissioner would be tasked with issuing best practice guidance to departments on a range of issues, including data minimisation, data encryption, the length of time appropriate for data retention and requirements for ensuring data security in public sector contractual arrangements with third parties.

Launch a Consultation with Industry on Data Security in the Private Sector

> *11. Task the Information Commissioner to carry out a consultation with the private sector, with a view to establishing guidance on data security, including examining the viability of introducing an industry-wide kite mark system of best practice.*

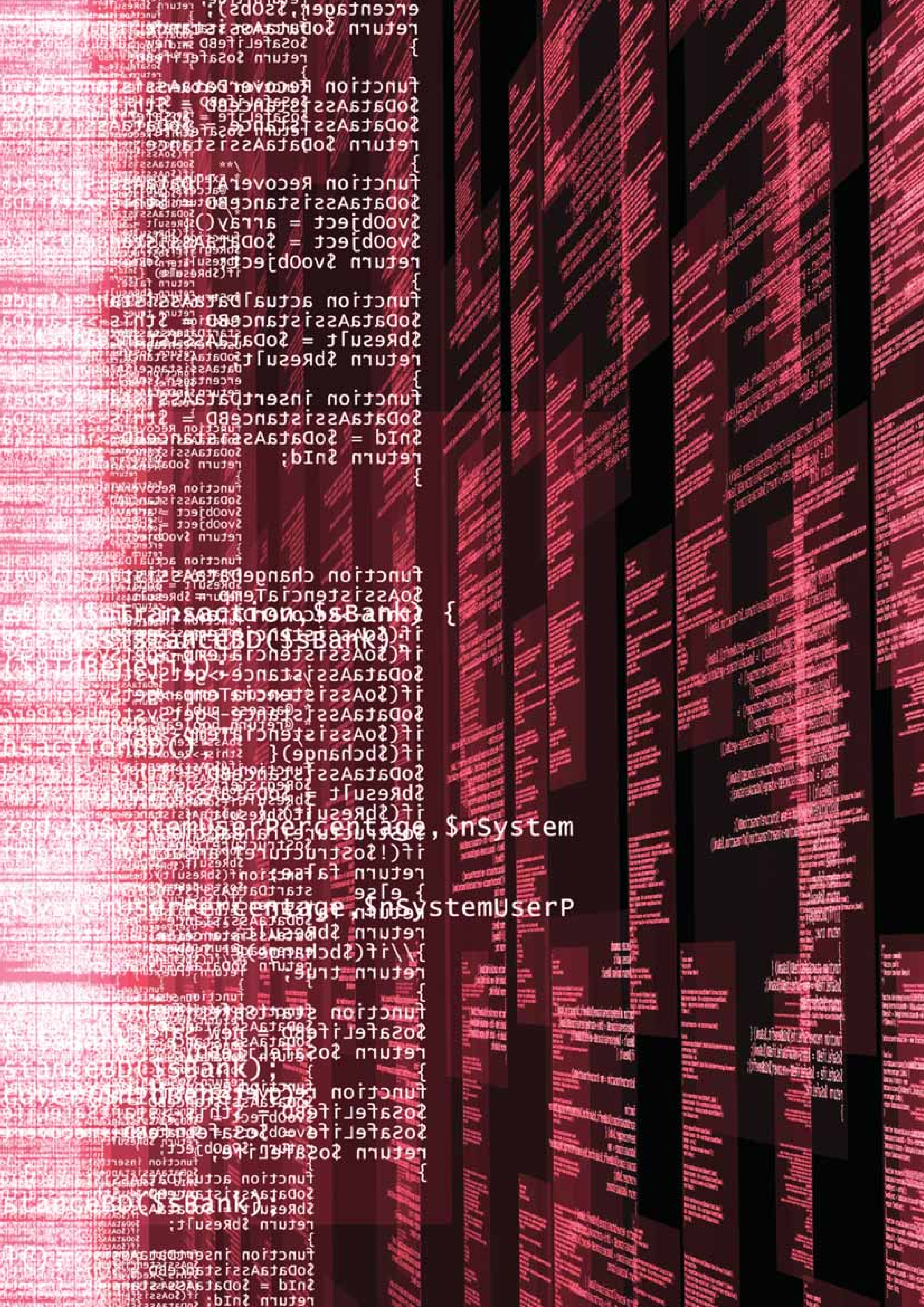
The focus of this report has remained data security in the public sector, in light of the growing concerns about the rise of a surveillance state. The relationship between the individual and the private sector is different. Data is more often shared on a voluntary – rather than coercive – basis and business is generally better at safeguarding personal data. However, there is increasing concern in this area, following high profile data breaches. In January 2009, it emerged that the online recruitment company, Monster, had been attacked by hackers who accessed a range of confidential information.[29]

In general, at least for commercial reputational reasons, companies have strong incentives to manage personal data securely and responsibly. However, the Data Protection Act is long and unwieldy. The Act informs organisations of their obligations, but offers little by way of guidance on how to go about securing this data. This presents a particular burden for smaller businesses.

As part of an ongoing review, we will engage in consultation with the private sector on further measures that are necessary and appropriate for data security. In particular, a Conservative government would task the Information Commissioner to consult with business on the viability of establishing an industry-wide data security kite mark, which would be voluntary but serve as a mark of best practice.

[1] Chapter 41, *Rasselas,* 1759
[2] Richard Thomas, Information Commissioner, interviewed in the *Times*, 16 August 2004.
[3] Press release, Information Commissioner, 2 November 2006.
[4] *Service Transformation: A better service for citizens and businesses, a better deal for the taxpayer*, Sir David Varney, published by HM Treasury, December 2006.
[5] Ibid, page 20.
[6] '2007 International Privacy Ranking', Privacy International, published on 28 December 2007
[7] ICM poll commissioned by the Information Commissioner. The Survey was conducted between 27 and 28 February 2008, with the results published in March 2008.
[8] *Independent*, 21 October 2008
[9] Reported widely, including *The Daily Telegraph*, 3 November 2008.
[10] For a comprehensive rebuttal of each argument in favour of ID cards, see *Identity Crisis – the Case against ID cards,* Peter Lilley MP, published by the Bow Group*,* February 2005.
[11] Reported in the *Times*, 6 August 2008.
[12] Tony McNulty, speech to IPPR, reported widely, including in the *Times*, 4 August 2005.
[13] See *Liberty*'s Response to the Home Office Document 'National Identity Scheme Delivery Plan 2008', June 2008.
[14] Oral evidence to the Home Affairs Select Committee, House of Commons, 8 June 2004.
[15] *The Scotsman*, 18 October 2005
[16] First reported, *Sunday Times*, 5 October 2008.
[17] *The Observer,* 8 March 2009.
[18] *Times*, 27 January 2009.
[19] *Database State*, Joseph Rowntree Report, 23 March 2009. Comments from Professor Anderson cited from the Joseph Rowntree press release of same date.
[20] Reported widely, including in the *Independent* and *Daily Mail*, 24 February 2009
[21] See the Reports of the Interception of Communications Commissioner for 2006 and 2007, published on 28 January 2008 and 22 July 2008 respectively.
[22] See paragraph 108, *Freedom of Information – one year on*, House of Commons Constitutional Affairs Committee, Seventh Report 2005-06.
[23] See the New Zealand Information Privacy Act 1993; and, in France, the operation of the CNIL (National Commission for Information and Liberties)
[24] Written answer from Tom Watson to the Parliamentary question from Francis Maude, *Hansard*, 15 January 2009.
[25] Paragraph 307.
[26] Cm 7449, July 2008, at page 24.
[27] The detail of a privacy impact assessment is explained in the Information Commissioner PIA Handbook.
[28] *The Observer,* 8 March 2009.
[29] Reported widely, including *The Guardian,* 27 January 2009.

Promoted by Alan Mabbutt on behalf of the Conservative Party both of 30 Millbank, London SW1P 4DP & printed by TPF Group, Avro House, Harlequin Avenue, Brentford TW8 9EW



function RecoverDataAssistance
return $oDataAssistance
function RecoverAllDataAssistance
$voObject = array()
return $voObject
function actualDataAssistance
$oDataAssistanceBD = $this->
$bResult = $oDataAssistanceBD
return $bResult
function insertDataAssistance
$oDataAssistanceBD = $this->
$nId = $oDataAssistanceBD->insert
return $nId;
function changeDataAssistance
$oAssistenciaTemp
($oTransaction,$sBank) {
if($oAssistenciaTemp
$oDataAssistance->getSystem
if($change){
$bResult =
$nSystemUserPercentage,$nSystem
return false;
} else
$nSystemUserPercentage,$nSystemUserP
return $bResult;
}//if($change)
return true;
function startSafeLife
$oSafeLifeBD = new
return $oSafeLifeBD
function RecoverSafeLife
$oSafeLife
return $oSafeLife;
function actualDataAssistance
$bResult =
return $bResult;
function insertDataAssistance
$oDataAssistanceBD = $this->
$nId = $oDataAssistance
return $nId;