Keeping control

We investigate whether the government and commercial companies can do more to protect your personal details

Most people in the UK will have their personal information stored in roughly 700 databases. For example, your bank, local authority and even online retailers will all hold your personal information. Other databases include supermarket loyalty schemes – Tesco Clubcard has around 10 million members, for example.

Almost every public and private organisation that holds personal information on a database must register with the Information Commissioner's Office (ICO) – one exception is if the database holds only the details of staff. All organisations that process personal data must comply with the UK's Data Protection Act, which means data needs to be secure and used appropriately.

It could take 300 hours to sort out your life after ID theft

Yet any weak link in the way these databases are managed and regulated can be catastrophic. If your personal information ends up in the wrong hands, for example, you can become a victim of fraud – we tell you how you can protect yourself against identity theft in our 'Checklist', opposite. And it's a nuisance to clear up: 300 hours is the best current estimate of how long it could take to sort out your life after identity theft. The Home Office Identity Fraud Steering Committee estimates that identity theft costs the UK £1.7 billion a year.

In this report, we scrutinise the way databases are managed and ask whether the government is doing enough to protect your personal details. We also look at how you can unknowingly put your privacy at risk on the internet, and give you advice on how you can protect yourself.

Enough protection?

Is the Data Protection Act protecting us properly? Not according to research carried out by law firm Pinsent Masons, which has its own data protection and privacy team.

When UK government ministers refused to disclose why the UK's Data Protection Act is under investigation by the European Commission, Pinsent Masons' Chris Pounder used the Freedom of Information Act 2000 to reveal that the Commission objects to the way the UK implemented 11 Articles of European data protection law – nearly one third of the entire Directive. The Commission's concerns focus on some of the most important aspects of data protection, including the powers given to the ICO.

Chris Pounder told us that the scale of the Commission's investigation indicates that the UK government may have tried to minimise the impact of legal obligations on

CALLER CONCERNS

Hundreds of public bodies have new powers to track your telephone use

In October 2007, public bodies were given the power to monitor use of the phone network, under the Regulation of Investigatory Powers Act 2000. These bodies won't know what was said in the call, but will be able to access data on every call made by every phone – including itemised phone bills and the names of people linked to these numbers. The police and security services will also be able to access where mobiles made or received specific calls. Data will be held by phone companies for 12 months.

Most people probably won't have a problem with the police using this data to, say, investigate terrorism and serious crimes. But the Home Office confirmed to us that more than 600 other public bodies – including local councils – will also have access to this information.

Given the number and severity of recent high-profile security blunders, the range of public agencies that will have access to the data has attracted much criticism.

These new laws may, however, be only the tip of the iceberg. The European Data Protection Directive, which underpins the new UK laws, wants member states to put in place data retention laws covering internet service providers by March 2009.

The Internet Service Providers' Association and privacy experts are now concerned this means that your emails, phone calls made over the internet and possibly even your internet surfing history may be logged and open to similar scrutiny.

PHOTOGRAPHY: ALAMY, PAUL FRANCIS, JOHN TRENHOLM

UNDER SURVEILLANCE

Are data protection laws keeping pace with new technology?

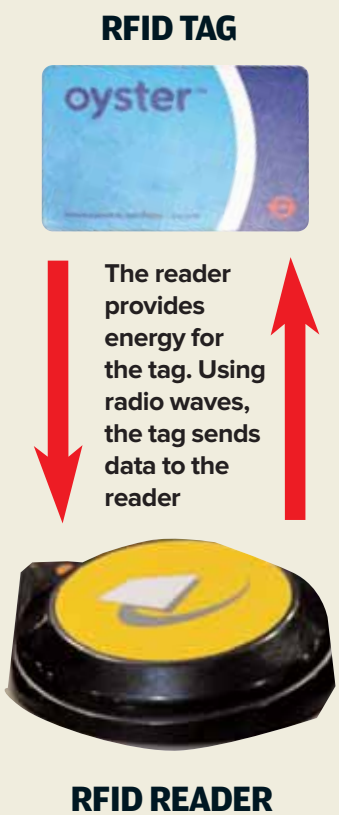
Radio frequency identification device (RFID) technology allows you to pay for things by touching, or being near, an RFID reader. RFID chips can carry information, such as personal details of a user, and are already in use. However, there are privacy concerns about some systems.

Transport for London's (TfL) Oyster card logs London tube and train passengers' travel details for eight weeks. The Information Commissioner states that RFID systems that link personal data with travel data should 'tell consumers what personal information is being collected, by whom, and for what purpose'.

Yet we discovered that when customers sign up for the Oyster card, all the registration data protection statement says is that the personal information is used for 'the purposes of administration, customer services and research'. It doesn't tell users that their journey data is recorded.

We also found that between January and October 2007 TfL received more than 3,100 police requests for passenger journey data.

We asked TfL how Oyster can comply with the Data Protection Act if it makes no reference to journey logging in its data protection statement.



TfL said the journey data is retained for 'administration and customer services'.

However, privacy lawyer Chris Pounder says the Data Protection Act insists people should be told why data about them is being collected.

TfL has also joined with O2, Barclaycard, Visa Europe, Nokia and AEG to trial a mobile phone that can be used like an Oyster card to pay for travel and allows users to make cashless payments in shops. We asked TfL how all of this personal information will be kept separate and secure by the six companies involved.

TfL said it doesn't have access to information on purchases and that it won't share travel data with these companies. It did say that these companies will share personal information, and that it has put in place 'a range of organisational and technological measures' to ensure customers' personal data is protected. We hope the databases will be secure – they will be exempt from ICO spot checks, as they're held by private companies.

database holders. As a result, the protection we're given by the Data Protection Act may be much weaker than it should be.

New powers

Following the HM Revenue and Customs (HMRC) fiasco last October, when personal data from 25 million people was lost, the government announced that it was giving the ICO new powers to do spot checks on public organisations and the way they manage their databases – powers the ICO has long sought. Yet these powers do not cover commercial organisations, such as supermarkets and their loyalty card schemes.

This is significant because, remarkably, the UK private sector is under no obligation to admit to security breaches. This means you may not be told if, say, your bank or mobile phone company loses your records.

The ICO told us that it would like compulsory laws on data breaches in the UK. In the meantime, it is calling for organisations to carry out 'privacy impact assessments' to better safeguard personal information and 'increase confidence' in data collection.

Loyalty cards

Some commercial databases, like the Tesco Clubcard loyalty scheme, are vast. The Clubcard has 10 million members and is estimated to generate an extra £100 million in annual sales. Tesco mails statements to its members quarterly – these statements contain tailored money-off vouchers and notices of discounts.

The ICO told us it would like compulsory laws on data breaches in the UK

Checklist

How to reduce your risk of identity theft and fraud

- **Credit awareness** Regularly check your personal credit file to make sure it's accurate. Use Call Credit, Equifax or Experian – see 'Contacts', p37, for more details. This costs £2 per company.
- **Monitor your money** Check bank and credit card statements to make sure there are no unfamiliar transactions. Cancel lost or stolen cards immediately.
- **Keep posted** Use a shredder to get rid of documents you don't need. Contact Royal Mail (0845 774 0740) if you suspect your mail is being stolen.

- **On guard** Never give personal or bank details to anyone who contacts you unexpectedly. Be suspicious, even if they claim to be from the police or your bank.
- **Online help** Don't use the same password for more than one account. Make sure you have up-to-date security software installed on your computer – see *Which?*, February 2008, p52.
- **Opt out** Don't tick 'yes' to share your details with third parties, and do tick the box on the electoral registration form that prevents your data from being accessed for marketing purposes .
- **Social networking** Give away only the minimum details and make sure you understand how to use the privacy settings. Go to www.ico.gov.uk/youth.aspx for more tips.
- **Unfair treatment** If you think your details are not being handled fairly, complain to the company. Contact the ICO if it's not resolved.

Tesco is able to do this because it can match the personal data of its members with every purchase they make. It then uses this information to build intricate profiles of people. Tesco told us that it never passes its customer data to other companies for commercial use.

If you like getting discounts off your regular purchases, great. But if you're uncomfortable about your supermarket monitoring your shopping habits, you may want to think twice about owning a loyalty card.

Companies are too vague

The ICO told us that organisations that collect personal data must ensure that individuals understand how their information will be stored and used, but data protection experts criticise the vague privacy statements used by some companies to justify their collection of personal data.

Professor Philip Leith from the School of Law at Queen's University Belfast told us that 'some statements don't tell consumers anything'. He points out that the Virgin Mobile privacy and security policy says that personal data is collected to 'develop your service for the future'. Yet the Virgin policy also says that your data may be shared outside the country and with other companies.

Virgin says it needs to share this personal information because it uses other companies to provide part of its service. However, Virgin itself appears to cast some doubt on whether those companies can keep your data secure, as its policy states: 'You should be aware that companies outside the European Union may have a lower standard of protection for personal information than that provided by the Data Protection Act 1998. We will, however, seek to have your data processed in accordance with English law.'

Search engine monitoring

When you use an internet search engine, you wouldn't expect it to keep track of which computer asked for the search, and which internet browser (software used to access the internet) and operating system (software that manages your computer) is used. But your searches may not be as private as you think.

For example, Google (www.google.co.uk) keeps this information – which isn't linked to your name – for 18 months, and then makes it anonymous by deleting the data

Some privacy statements don't tell consumers anything

PERSONAL INFORMATION GOING OVERSEAS

Rod Davis *29*

Rod Davis, from Cheshire, was a customer of Lloyds TSB's shares dealing and management business. Lloyds sold the company in July last year and it was renamed the Equiniti group.

In September 2007, Rod received a letter that said new terms and conditions for the service applied, namely that 'Equiniti Limited will be able to send your data outside Europe in some circumstances (for instance to India or the USA)'. The more detailed terms on the company's website added that the data protection laws and standards might differ in those countries but the company would continue to be strictly bound by the UK's Data Protection Act.

Unhappy with this clause, Rod wrote to Equiniti stating that he wished to remain a customer but did not give permission for his data to be transferred outside the UK. To Rod's surprise, Equiniti closed his account.

After further correspondence, Equiniti reopened Rod's account and said his data protection request had been 'actioned'.

Equiniti told us: 'The change to the terms and conditions, which allows us to transfer data overseas, is within the UK Data Protection Act.'

Check your terms and conditions to make sure you are happy with the way your data will be used. If you're not, complain – see 'Checklist', p35, for more. You could also swap to a company that has terms you are happy with.

Internet safety

Fraudsters can target those who reveal too much online

Crooks can use the internet to gather information about people, and then use this knowledge to trick people into giving away Pin details, passwords or other security information.

'They can build up an impressively detailed picture by accumulating small bits of data,' says the National Hi-Tech Crime Unit. 'This can make them seem even more plausible when they make their move.'

There may be more information about you online than you think, as *Which?* editor Neil Fowler (right) discovered.

Revealing details

Neil challenged us to find out as much as possible about him online. All our researcher had to go on was Neil's name and occupation. We found:

- Neil's close family's names.
- His full address.
- The value of the house he bought and the price paid by the previous owners, and their names.
- The names of his neighbours.
- The floorplans to his home, which include access points, plus a detailed satellite image of his home and garden.

All of this information was available on publicly accessible websites. Although Neil is a public figure, this isn't why we were able to track down information about him. By using the internet, fraudsters could find out information about lots of us – particularly if you reveal too much about yourself on social networking sites.

that links it to individual computers. We asked Google why it needed this information on its users, and why it kept it for 18 months. Google said: 'This information helps us to improve our systems. We feel that this length of time is the right balance between protecting our users' privacy and keeping a secure system.'

To help anonymise your searches, regularly delete your cookies – files saved on your computer's hard disk that tell a website whether you've visited it before. Go to our website at www.which.co.uk/onlineID to find out how.

What currently happens

Dr David Murakami Wood, a lecturer at Newcastle University and joint editor of a major report commissioned by the ICO on surveillance and privacy, told us that the government and many large companies don't understand how valuable personal information on databases is: 'They still think that computer databases are the equivalent of paper files – just some numbers that help them get their jobs done. They have no awareness of just how vital this data is for people's futures. And this awareness needs to be hammered home to government.'

Privacy expert Chris Pounder stresses that the current system of data protection regulation depends on people complaining to the ICO if they think their data is not being processed fairly. He urges people to do so – see 'Contacts', right, for details.

Which? says

Well-publicised data security debacles include HMRC losing the bank details of 25 million people, personal details of three million learner drivers being lost and nine NHS trusts in England losing patient records – including one trust losing the personal details of 160,000 children. But even before this, the public was concerned about data protection – ICO research in September 2007 found that 60 per cent of people in the UK thought that they had lost control over the way their personal information is collected and processed.

Yet despite the severity of the security problems so far made public, the government is pressing ahead with a range of new databases, including one that will list every child in Britain. In its defence, the government has launched a consultation into how personal information is shared in the public and private sectors. This will examine whether information is circulating too freely.

It would also be good to see the government consider whether it should extend the ICO's powers to carry out spot checks on private sector databases, and to force all organisations to notify their customers and the ICO about security breaches.

As a result of our investigation, we are concerned that Virgin and Transport for London are not complying with the Data Protection Act, so we urge them to tighten up their processes.

NETWORKING NOUS

If you're not careful on social networking sites, you could end up revealing your personal details to people all around the world

While internet trends come and go, few have rocketed in popularity in the way social networking did in 2006 and 2007. For example, Bebo (www.bebo.com) claims it has 11.9 million users in the UK; Facebook (www.facebook.com) claims seven million.

But as the sites have grown in popularity, so have concerns about privacy. For example,

after receiving a complaint from a member of the public, the Information Commissioner's Office is currently investigating why personal information remains on Facebook's computers after a user deactivates their account. And our investigation has found that the profiles of hundreds of thousands of Bebo and MySpace (www.myspace.com) users are accessible to anyone via the search engine Google (www.google.co.uk). Bebo is targeted at 13- to 24-year-olds.

Sort out your settings

Users of Facebook can also inadvertently put their privacy at risk. When users set up an account with Facebook they can join networks of other users – for instance, there are two million people in the London network.

The default privacy setting means everyone in the networks you join can see your profile, which can include your date of birth, sexuality, contact details and links to your family and friends.

Internet security firm Sophos states: 'As networks can contain hundreds of thousands of people – and you have no control over who else joins the network – you are instantly revealing personal information to potential identity thieves if you leave this option at its default setting.'

Facebook told us: 'Facebook encourages users to customise their security settings to a level they are comfortable with.'

Sites need to improve

However, Facebook and rival sites Bebo and MySpace have all been criticised because their security settings are difficult to use. User Vision is one of Europe's leading web usability consultancies. Its recent audit of the three sites found that 'all lacked targeted, clear information about online security for under-18s'. User Vision's Strategic Director, Emma Kirk, says that it is no good having privacy settings if users find them difficult to use.

Facebook said that it encourages people to use their privacy settings and does provide security tips. But Emma Kirkland says the site doesn't go nearly far enough.

See our 'Checklist', p35, for more information about how you can protect your details on social networking sites.

Contacts

Call Credit 0113 244 1555
www.callcredit.co.uk

Equifax www.equifax.co.uk

Experian 0844 481 8000
www.experian.co.uk

Information Commissioner's Office
01625 545745
www.ico.gov.uk

Safety advice

Bank Safe Online
www.banksafeonline.org.uk

Get Safe Online
www.getsafeonline.org

Home Office: identity theft
www.identity-theft.org.uk

UK Fraud Prevention Service
www.identityfraud.org.uk