



# Latest ISEB results

We are pleased to announce our latest results for the ISEB Certificates in Data Protection and Freedom of Information.

Once again Act Now candidates achieved excellent results, with only five fails out of the 25 candidates who sat the January exams. Please see below a summary of all our results so far.

|              | Delegates | Passes | Pass rate (%) | Average pass mark |
|--------------|-----------|--------|---------------|-------------------|
| <b>FOI</b>   | 23        | 21     | 91.3          | 60.85             |
| <b>DP</b>    | 17        | 13     | 76.5          | 60.65             |
| <b>Total</b> | 40        | 34     | 85.0          | 60.75             |

On FOI we are achieving a success rate of 91.3%. This is well above the rate for all providers for 2007/08, which stands at 81% (as stated on the ISEB website).

Our next courses are in Edinburgh and London in June. Please see our website for details and a list of successful candidates:

[www.actnow.org.uk/content/29](http://www.actnow.org.uk/content/29)

These courses are ideal for those who wish to have their knowledge and expertise recognised through a formal qualification. We aim to achieve a 100% pass rate. With this in mind we have built into the programme a day for a mock exam and revision. Delegates will receive a comprehensive set of materials (including copies of all legislation and

codes) and also be kept in touch with the course tutor to discuss exam preparation, revision, homework and exam technique.

Delegates' commented:

"A well-structured and well timed course. The course itself and the knowledge of the trainer have really helped me to improve my knowledge and understanding of the Freedom of Information Act and will be extremely useful to me in my job at the council."

**Ed Zerafa, Peterborough City Council**

"I'd just like to state that I enjoyed the course, found it informative and a great help in relation to my FOI Officer functions. You were very supportive in all aspects of the course and the course was also a good opportunity to meet fellow FOI officers and discuss work-related issues."

**Tony Fitzpatrick, Mersey Travel**

"The course was well structured and paced and covered all the key issues in some depth!"

**Iain Harrison, Coventry City Council**

### EDINBURGH

In June we are running our first ISEB accredited FOI/FOISA course in Edinburgh. This will teach delegates about both Acts but there will be a focus on the Freedom of Information (Scotland) Act 2002. It is ideal for Scottish FOISA practitioners who wish to have their expertise recognised through a formal qualification.

Spaces are already filling up, so please book early to avoid disappointment. More details at:

[www.actnow.org.uk/content/29](http://www.actnow.org.uk/content/29)

## WELCOME

to our 38th Newsletter – probably the newsletter with the largest circulation in the sector, with 6,067 subscribers, published every quarter and now entering its 10th year. Previous issues are archived on our website.

### In this issue:

#### FREEDOM OF INFORMATION

3. Access to the files of the deceased
4. FOI resources

#### DATA PROTECTION

6. £500k fines for DP offences
7. Report breaches, warns the ICO

#### SURVEILLANCE LAW AND PRIVACY

10. Part 2 of RIPA: The new law

And much more...

Previous issues are archived on our website.

This newsletter contains links to other websites. We cannot be responsible for content or availability of other sites. Please read the notice at the end of this newsletter.

**Next issue: June 2010**





Freedom of information

# FOI v DPA

The tax status of Lord Ashcroft, the Conservative Party's major donor and deputy chairman, has been the subject of much controversy over the past few years. Lord Ashcroft gave an undertaking to the government in March 2000 to end his status as a tax exile (or "non-dom") when he received a life peerage. This undertaking was the subject of a recent FOI request to the Cabinet Office by a Labour MP.

Gordon Prentice requested disclosure of the form in which the undertaking was given and the identity of the person who received it. The Cabinet Office confirmed it held the information but determined that it should be withheld in reliance of the exemptions contained in sections 37(1) (b) (the conferring of honours), 40(2) (personal data) and 41 (Breach of Confidence). All these exemptions require consideration of the public interest in disclosure.

The Commissioner decided that the Cabinet Office was wrong to rely on the exemptions (Cabinet Office Ref:

FS50197952 28/01/2010). He ruled that there was a legitimate public interest in knowing whether Lord Ashcroft has actually fulfilled the undertaking. In the Commissioner's view the public interest in transparency in the honours system outweighed the Cabinet Office's claim that disclosure would be "unwarranted and prejudicial to the rights and legitimate interests" of Lord Ashcroft.

This is an interesting case, not just because of its political angle in the year of an election but because the Commissioner has ruled that personal data is disclosable under FOI to a third party, even though it could not be requested by Lord Ashcroft himself by making a subject access request under section 7 of the Data Protection Act 1998 (DPA). This is due to the exemption in the DPA for personal data processed for the purpose of "the conferring by the Crown of any honour" (schedule 7).

Paul Simpkins is running our ever popular course on handling requests for personal data. It is held across the UK and covers how to handle requests for personal data under both FOI and the DPA.

More details:  
[www.actnow.org.uk/courses/Data\\_Protection](http://www.actnow.org.uk/courses/Data_Protection) ■

Freedom of information

# 2nd veto

Section 35 allows information to be withheld if it relates to, among other things, the formulation or development of government policy. It has been the subject of two decisions which have gone on to be vetoed by the government using its powers under section 53 of the Act.

In *Cabinet Office and Dr Christopher Lamb v IC* (EA/2008/0024 & 0029 27 January 2009) the Tribunal upheld the ruling by the Information Commissioner that minutes of Cabinet meetings from 2003 should be released. These refer to meetings that discussed the Attorney-General's legal advice about the Iraq war. On 24 February 2009 Lord Chancellor Jack Straw issued the first ever ministerial veto under section 53 of the Act.

The Commissioner said at the time: "Anything other than exceptional use of the veto would threaten to undermine much of the progress towards greater openness and transparency in government

since the FOI Act came into force."

Unfortunately these words seem to have fallen on deaf ears. On 10 December 2009, Mr Straw announced that he was exercising his powers of veto for a second time. The new veto has been issued in respect of a decision of the Commissioner (Cabinet Office FS50100665 23/6/09) requiring disclosure of minutes of the Cabinet Ministerial Committee on devolution to Scotland and Wales and the English Regions in 1997. Mr Straw stated that disclosure of the information would have put the convention of collective Cabinet responsibility at serious risk of harm. He also stated that he considered the circumstances of the case to be exceptional. Interestingly these are the same reasons given by him when exercising the veto for the first time.

The effect of the veto is that the original decision notice ceases to have effect. The Commissioner has expressed concern that the veto was issued even before allowing the Tribunal to rule on the Cabinet Office's appeal. This is in stark contrast to the Iraq minutes case (discussed above), where the veto was issued after the Tribunal's decision. ■

## CONTENTS

### FREEDOM OF INFORMATION & EIR

3. Access to the files of the deceased
4. Disclosure of university course materials
4. FOI resources
5. FOISA in Scotland
5. UK FOI in brief

### DATA PROTECTION

6. £500k fines for DP offences
7. Report breaches, warns the ICO
7. Information security workshop
8. DP news roundup
9. Data Protection Helpline

### RIPA & SURVEILLANCE

10. Part 2 of RIPA: The new law
10. RIPA Forms Guidance Manual (version 3)
11. RIPA/RIPSA helpline
12. Surveillance news roundup



Freedom of information

# Access to files of the deceased

When it comes to considering requests for information about the deceased, two recent decisions of the Information Commissioner have emphasised the importance of checking whether the requestor is the deceased's appointed personal representative. If they are not then the disclosure could be an actionable Breach of Confidence and so the section 41 exemption will apply. This is the case even if the applicant is the next of kin.

In a decision involving Coventry City Council (FS50213780 21/12/ 2009), Coventry Law Centre (CLC), acting on behalf of the complainant, made an information request for copies of social services files relating to the complainant and her husband, who was deceased. The council considered that the request for the complainant's file was a subject access request under the Data Protection Act 1998 and it provided this information. However, it refused to provide any of the information held on the complainant's husband's file because it considered that this information was exempt under section 41.

The Commissioner found that both exemptions had been correctly applied. With regard to section 41, he held that the council owed a duty of confidence to the deceased which would be capable of surviving the complainant's husband's death even though it appeared that there may not have been any personal representative appointed to manage his affairs. This is because there is always the possibility that a personal representative could be appointed following the disclosure and could take action against the council for a Breach of Confidence. The fact that the complainant was the wife of the deceased was immaterial as she had never applied to become the personal representative upon his death.

In order to decide that a Breach of Confidence is actionable, the Commissioner had to consider the applicability of the inherent public interest defence. The Commissioner recognised that it is in the public interest to bring to light any wrongdoing on the part of public authorities



and for individuals to have access to information to help them to conduct a case. However, it was not apparent to the Commissioner that there has been any proven wrongdoing on the part of the council and he also noted that if the complainant did pursue a negligence claim, information may be accessible through court disclosure rules. He also noted that it is likely that the complaint could be reviewed by other independent bodies with the jurisdiction to consider such issues. He therefore took the view that the public interest in preserving the principle of confidentiality is much stronger in the circumstances of this case and that there would therefore be no public interest defence available if the council had disclosed the information.

A similar decision was reached by the Information Commissioner when a request was made for the social services records of a deceased service user to Leicestershire County Council (FS50213781 22/12/2009). Here the Commissioner relied on the fact that the complainant had stated that both she and her brother were appointed as personal representatives of the deceased in May 2009 and were given letters of administration. The complainant's

brother had objected to the disclosure of information to her. The Commissioner therefore ruled that section 41 applied because the complainant's brother, or any other personal representative that may be appointed in the future, could bring a claim against the council for Breach of Confidence.

These cases emphasise the importance of public authorities checking the status of the applicant and asking whether he or she is really the personal representative of the deceased whose information is being requested. If he/she is not the personal representative then, even though they may be close family, any disclosure could lead to the public authority being sued by the personal representatives for Breach of Confidence.

The web has many videos that touch on this area. It appears that gory photos of a dead person can be posted by anyone and that these posters have immunity because of freedom of expression. The deceased has no rights. Worrying stuff:

<http://tinyurl.com/y9yez4c>

Please see Ibrahim Hasan's article on dealing with requests for information about the deceased:

[www.informationlaw.org.uk/page16.htm](http://www.informationlaw.org.uk/page16.htm)



Freedom of information

# Disclosure of course materials

In a recent decision, the Information Tribunal considered the question of whether FOI can be used to gain access to university course materials. In

<http://tinyurl.com/ya9v39s>

*University of Lancashire v IC* (EA/2009/0034 18 December 2009) it had to balance the commercial interests of the university with important matters of public interest in knowing what is being taught at a publicly funded institution. The university had earlier refused a request for disclosure of course materials relating to a BSc degree course in homeopathy. As well as section 36, the university had claimed the section 43 exemption, that disclosure of the course materials would damage its commercial interests.

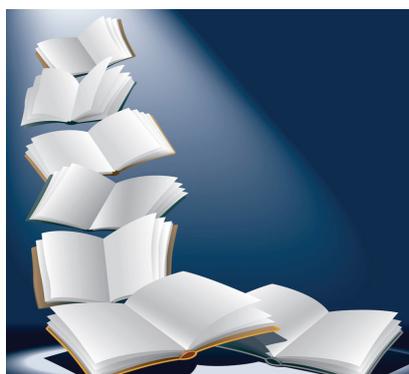
At first instance, the Information Commissioner held that the university should have disclosed the course materials, except certain elements, and particularly empirical case studies, which could be withheld under the section 41 exemption (where disclosure would lead to an actionable breach of confidence). The Tribunal agreed with the Commissioner and dismissed the university's appeal. It had argued before the Tribunal that the course materials were exempt from disclosure because they contained a

significant amount of third party copyrighted information and disclosure of that material would discourage third parties from contributing to course materials in the future. The Tribunal rejected these arguments, stating that disclosure of information under FOI would not in any way

have diluted any copyright enjoyed by the third parties and there was, in any event, no sufficient evidence before the Tribunal to substantiate the university's case that disclosure of the copyrighted material would have had an alienating effect on third party contributors.

The Tribunal also found that there were strong public interests in members of the public being able to test the educational value of publicly funded degree courses and in accessing information relating to a homeopathy degree course, which was a controversial subject. This is an important case which

will have a big impact on universities seeking to restrict access to educational resources for various reasons. It also emphasises that copyright in itself cannot be used to withhold information under FOI. An earlier decision by the Information Commissioner involving the Student Loans Company Ltd (Case Ref: FS50217416 04/02/2009) came to the same conclusion. ■



Freedom of information

# FOI resources

For the latest news analysis and comment on freedom of information please have a look at the following resources on our websites:

[www.actnow.org.uk](http://www.actnow.org.uk)

[www.informationlaw.org.uk](http://www.informationlaw.org.uk)

**UK PODCAST:** If you would like a full explanation of all the latest FOI decisions then listen to the FOI podcast from Ibrahim Hasan. This is the first service of its kind in the UK and it's completely free. It's even been mentioned in *The Times*.

Every month Ibrahim discusses the latest legal cases and gives his personal views as to how they affect FOI

practice. The first 19 episodes are now on Ibrahim's personal website together with the scripts. See:

[www.informationlaw.org.uk/page20.htm](http://www.informationlaw.org.uk/page20.htm)



**WEBCAST:** Act Now also runs the information/surveillance law webcast series. This is free to attend. All you need is a computer and a set of headphones. You can listen to Ibrahim's web seminar and ask questions live. You can also view previous web seminars. More details:

[www.actnow.org.uk/content/50](http://www.actnow.org.uk/content/50)

**ARTICLES:** Ibrahim also writes a regular FOI Update column for the *Law*

*Society Gazette*. You can read this at:

[www.informationlaw.org.uk/page16.htm](http://www.informationlaw.org.uk/page16.htm)

**WORKSHOPS:** Our speakers will be covering these and other developments in forthcoming FOI Update workshops in Bristol, Belfast and Edinburgh:

[www.actnow.org.uk/courses/Freedom\\_of\\_Information](http://www.actnow.org.uk/courses/Freedom_of_Information)

**FOI HELPLINE:** Act Now training provides an FOI Helpline service. This is designed to supplement your internal FOI expertise by acting as a "sounding board" or "signpost service" for you to discuss your FOI/EIR requests and possible responses. Through the helpline I will be available to guide you through the relevant area of law, discuss possible exemptions and how to deal with any complaints. At a time of increasing pressure on public sector budgets, the Act Now FOI Helpline is the most cost-effective solution for your FOI problems. More details at

[www.actnow.org.uk/content/25](http://www.actnow.org.uk/content/25) ■



Freedom of information

# FOISA in Scotland

## S.60 Code Consultation

The Scottish Executive has just completed a consultation on a revised code of practice under section 60 of the FOI (Scotland) Act 2002. Details can be found at:

▶ <http://tinyurl.com/yzqx9en>

The section 60 Code of Practice on the Discharge of Functions by Public Authorities provides guidance to Scottish public authorities on practices they should follow in meeting their FOI obligations.

The current section 60 Code of Practice is available at:  
▶ <http://tinyurl.com/ygqm5e7>



## Extension of FOISA?

On 8 December 2009 the Scottish government announced that it plans to consult on whether the Freedom of Information (Scotland) Act should be extended to the following bodies:

- Contractors who build and maintain hospitals
- Contractors who build and maintain schools
- Contractors who run privately managed prisons and provide prisoner escort and court custody services
- Contractors who operate and maintain trunk roads under private finance contracts
- The Glasgow Housing Association
- The Association of Chief Police Officers in Scotland and
- Bodies used by local authorities to provide leisure, culture and sport services.

A report containing the Scottish government's response to the earlier discussion paper on the subject has also been published:

▶ <http://tinyurl.com/yjwwmkc>

A Scottish government news release is at:

▶ <http://tinyurl.com/yjr8xtm>

and an SIC release is at:

▶ <http://tinyurl.com/yekyj2h>

## SIC Newsletter

Read Kevin Dunion's latest FOISA newsletter and his annual report for 2009, which is being offered electronically for the first time and includes video and interactive tables. The theme is "You only have to ask":

▶ [www.itspublicknowledge.info](http://www.itspublicknowledge.info)

## Courses in Edinburgh

Act Now has a full programme in Scotland on DPA, FOISA, RM and RIPSAs:

▶ [www.actnow.org.uk/courses/city\\_Edinburgh](http://www.actnow.org.uk/courses/city_Edinburgh)

We will also be running the ISEB Data Protection and Freedom of Information Courses in Edinburgh in 2010. ■

Freedom of information

# UK FOI in brief

## New Tribunal

On Monday 18 January 2010, the Information Tribunal ceased to exist. All its work has been transferred to the new General Regulatory Chamber. From 18 January, all FOI appeals will be heard either in the First-tier Tribunal (Information Rights) or in the Upper Tribunal. The question as to where each appeal will be heard will be determined by two new sets of Tribunal rules as well as practice directions.

In respect of appeals commenced prior to this date, the Tribunal will have discretion as to whether to apply the old rules or the new rules, or a combination of the two.

## Disclosure of FOI requests

*The Scotsman* reports that Moray Council has become the first in Scotland to put every FOI request it receives, and the responses, on its website. Private details of the requester are withheld. See the headline "Tartan Transparency":

▶ <http://tinyurl.com/yznls88>

However, Bexley Council is going even further by naming FOI requestors!

▶ <http://tinyurl.com/ygmmk3n>

Would this not be a breach of the DPA? We wonder if this will catch on.

## Climate Row

A university unit involved in a row over stolen emails on climate research breached rules by withholding data, the Information Commissioner's Office has said:

▶ <http://tinyurl.com/yjbomkw>

## ICO newsletter

The latest edition of the Information Commissioner's newsletter can be read on his website:

▶ <http://tinyurl.com/y8jd963>

## New websites

Openly Local is a new project to develop an open and unified way of accessing local government information:

▶ [www.openlylocal.com](http://www.openlylocal.com)

Web founder Sir Tim Berners-Lee has unveiled his latest venture for the UK government, which offers the public better access to official data. A new website will offer reams of public sector data, ranging from traffic statistics to crime figures, for private or commercial use. The target is to kickstart a new wave of services that find novel ways to make use of the information. See:

▶ <http://data.gov.uk>

and the BBC story at:

▶ <http://tinyurl.com/y946tpk> ■



Data protection

# Fines of £500,000 for data protection offences

New powers, designed to deter personal data security breaches, are to come into force on 6 April 2010. The Information Commissioner's Office (ICO) will be able to order organisations to pay up to £500,000 as a penalty for serious breaches of the Data Protection Act 1998 (DPA). The penalties for serious data protection breaches have been approved by the government.

The power to impose a monetary penalty notice is designed to deal with serious breaches of the DPA and is part of the ICO's overall regulatory toolkit, which includes the power to serve an enforcement notice and the power to prosecute those involved in the unlawful trade in confidential personal data.

The level of the fine will be determined after an investigation to assess the gravity of the offence. Other factors that will be considered will include the size and the financial

resources of the organisation found to be in breach of the law. The Information Commissioner will consider the circumstances, including: the seriousness of the data breach; the likelihood of substantial damage and distress to individuals; whether the breach was deliberate or negligent; and what reasonable steps the organisation has taken to prevent breaches.

A statement from the Information Commissioner, Christopher Graham, said: "These penalties are designed to act as a deterrent and to promote compliance with the Data Protection Act. I remain committed to working with voluntary, public and private bodies to help them stick to the rules and comply with the Act. But I will not hesitate to use these tough new sanctions for the most serious cases where organisations disregard the law."

The ICO has produced statutory guidance on how it proposes to use this new power. ■





Data protection

# Report breaches, warns the ICO

Over 800 data security breaches have been reported to the Information Commissioner's Office (ICO) in just over two years, the privacy watchdog has announced. The ICO is warning that organisations may face tougher sanctions if they fail to report breaches which subsequently come to light.

David Smith, Deputy Commissioner, said: "In just over two months a further 100 organisations have reported data security breaches to us. We are keen to work with organisations to prevent breaches occurring in the first place and to help put things right when things do go wrong. Talking to us may, of course, result in regulatory action. However, organisations must act responsibly; those that try to cover up breaches which we subsequently become aware of are likely to face tougher regulatory sanctions."

Mistakes account for 195 of the 818 data security breaches reported to the ICO since November 2007. 262 are the result of theft, often where the personal information was held on an unencrypted portable device. The ICO gives free advice to organisations to help them comply with the Data Protection Act (DPA). Organisations can minimise the risks of security breaches involving personal information by ensuring that all portable media devices containing personal information are encrypted. Staff must be adequately trained and organisations should give proper consideration to restricting staff from downloading large volumes of data onto memory



sticks and other portable devices. All personal information held in buildings and offices should be protected by adequate security arrangements to prevent theft or the loss of the data. The loss of personal information can cause individuals harm and distress. It can also lead to reputational damage and loss of customer trust for organisations.

New powers to deter breaches should come into force on 6 April 2010. The ICO will be able to order organisations to pay up to £500,000 as a penalty for serious breaches of the DPA. The power to impose a fine is designed to deal with the most serious personal data breaches and is part of the ICO's overall regulatory toolkit, which includes the power to serve an enforcement notice and the power to prosecute those

involved in the unlawful trade in confidential personal data. The ICO has produced the *Plain English Guide to Data Protection* at:

<http://tinyurl.com/yanmo29>

This provides businesses and organisations with practical advice about the DPA. The guide is intended to help organisations safeguard people's personal details and comply with the law. The guide takes a straightforward look at the principles of the Data Protection Act and uses practical, business-based examples.

A copy of the breach table is available here:

<http://tinyurl.com/yf4vljg>

Data protection

## Info security workshop

One of the central government responses to data breaches is to align its security activity with ISO27001 more fully and reframe its security policy. Our new course will look at what that means in practice and how it affects the wider public sector, introducing the Seven Principles of the HMG SPF and aligning them with current information security, assurance and governance trends and requirements.

This revised workshop is facilitated by legal

and information security expert Andrea Simmons and is designed to cut through the jargon and media hype. It will give delegates the knowledge to write their own action plan for bringing information security into their organisation. The legal and regulatory regime will be discussed as well as the practical options to prevent loss, damage and destruction of confidential/personal information. Details:

[www.actnow.org.uk/courses/417](http://www.actnow.org.uk/courses/417)





## Data protection



## To share or not to share...

The South West Information Compliance Group's (SWICG's) Annual Seminar on Data Sharing takes place on Wednesday 26 May 2010. Ibrahim Hasan will be speaking at this event. More details:

[www.swicg.org.uk](http://www.swicg.org.uk)

## Bristol courses

Act Now is running Data Protection and Information Sharing Courses in Bristol with Philip Bradshaw. For more information please see:

<http://tinyurl.com/ygdh8r9>

Or download a colour flyer here:

<http://tinyurl.com/yjcjopn>

## Data theft at HSBC

About 24,000 clients of HSBC's private banking operation in Switzerland had personal details stolen by a former employee, the company has admitted. In December, HSBC said that just 10 account holders were affected by the theft, which happened three years ago. The information stolen concerns 15,000 accounts that are still active. Another 9,000 accounts have been closed since the theft.

<http://tinyurl.com/ya6a7st>

## Offender alerts

A scheme allowing parents to check if someone is a sex offender will be rolled out across England and Wales by March 2011, the Home Office says.

A year-long pilot has already protected 60 children, ministers say. A similar scheme is to be launched in Scotland.

<http://tinyurl.com/yjk4bpd>

## Labour in breach of PECR

The BBC is reporting that the ICO has served an enforcement notice on the Labour party for breaching PECRs by making automated phone calls to nearly 500,000 people. See:

<http://tinyurl.com/yg8e396>

## Chips in bins

Privacy campaigners claim increasing numbers of councils are gearing up for "pay as you throw" rubbish charges by installing microchips in wheelie bins. The Big Brother Watch group says its survey found 68 UK authorities with the technology at their disposal – up from 42 last year – with chips in 2.6 million bins.

<http://tinyurl.com/yh9sxoe>

## New CCTV cameras

CCTV cameras that can pick out abandoned luggage and suspicious behaviour and which can lock onto potential suspects are being developed by UK researchers. It is hoped the technology could help prevent terrorist attacks by spotting odd elements in a situation before it can escalate.

<http://tinyurl.com/y9fsb5e>

## 101 uses for a dead NINO

You thought it was only payroll, pensions and maybe ISAs but there are

dozens of lawful uses for your National Insurance Number. Check out:

<http://tinyurl.com/yglo5x8>

## Mobile phone spying



Software on mobile phones can be used to track the owner's every move and listen in on every phone call. It costs as little as \$50. Watch the video on our website under "Surveillance Videos":

[www.informationlaw.org.uk/page21.htm](http://www.informationlaw.org.uk/page21.htm)

We know it's a criminal offence and hopefully the courts, the ICO and "uncle Tom Cobley and all" would throw the book at the perpetrators but, if it is this easy, why is every journalist not using this software? Or are they? See also:

<http://tinyurl.com/yg8qldm>

## Medical confidentiality

When does a doctor's duty of confidentiality to their patient end? The revelation that Mo Mowlam deceived Tony Blair, her own family and most of the country about the seriousness of that brain tumour before the 1997 election that made her Northern Ireland Secretary is a fascinating study in the power of myth.

See:

<http://tinyurl.com/y194eyp>

Documentation Sciences Foundation has a web page with links to videos about the basic rights that individuals have under the Universal Declaration of Human Rights. The one about privacy (article 12) is rather cool. Some of the others are a bit schmaltzy but definitely worth a look. See:

<http://tinyurl.com/yg9ob4a>



Data protection

# Data Protection Helpline

The Act Now DP Helpline is designed to supplement your internal expertise by acting as a friendly advisor with whom you can discuss your data protection and privacy issues and avoid attracting the attention of the Information Commissioner.

Our experts will guide you through the relevant sections of the Act and make recommendations about your response to difficult DP situations.

Public authorities are increasingly receiving complex and time-consuming data protection requests. These involve consideration of a number of data protection

exemptions as well as relevant Information Commissioner and Information Tribunal decisions. Internal legal departments are often over-stretched and dedicated data protection practitioners are hard to recruit.

External legal advice in this area is very expensive and there are very few experts in this field with real experience of advising the public



sector.

Please click here for more information and subscription details:

[www.actnow.org.uk/content/25](http://www.actnow.org.uk/content/25) ■





Surveillance law and privacy

# Part 2 of RIPA: The new law

Three new orders, under Part 2 of the Regulation of Investigatory Powers Act 2000 (RIPA), came into force on 6 April 2010. The orders are designed to ensure that covert surveillance techniques can continue to be used by public authorities when they are necessary and proportionate, but that there is no repetition of the small number of recently reported cases where they have been used in a disproportionate manner. Examples include local authorities conducting covert surveillance on parents to check their stated address on school application forms and on dog owners to ensure they comply with dog-fouling laws.

The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 consolidates four previous orders relating to covert surveillance and the use or conduct of a covert human intelligence source (CHIS) by public authorities. It sets which authorities can use such surveillance techniques, on what grounds and who has to authorise their use.

The new order revises the prescribed officers for local authorities who can sign authorisations (known as “authorising officers”) to “Director, Head of Service, Service Manager or equivalent”. Previously this was set at “Assistant Chief Officer, service manager or equivalent or any more senior officer”. This led to criticism by the Office of Surveillance Commissioners (OSC) that more junior officers were authorising surveillance and getting it wrong. The new provisions (and the explanations on the Home Office website) suggest that all local authorities should revise their list of authorising officers to include only directors or their equivalent.

The Regulation of Investigatory Powers (Covert Surveillance and Property Interference: Code of Practice) Order 2010 and the Regulation of Investigatory Powers (Covert Human Intelligence Sources:

## RIPA Forms Guidance Manual (version 3)

Act Now Training is pleased to announce that version 3 of the RIPA Forms Guidance Manual has now been published. It has been fully revised in the light of the new RIPA Order and Codes of Practice, which came into force on 6 April 2010. The Home Office forms still make reference to the old codes. Our forms are reproduced with references to the new codes.

Version 3 (April 2010) of the Guidance includes each RIPA form with:

- Detailed notes on how to complete each section
- References to the new RIPA Codes and Order
- References to the OSC Procedures and Guidance Document

Other useful documents including:

- A detailed briefing note on the new RIPA codes and the changes they make to the local authority RIPA regime
- Revised colour flowcharts to help officers decide what type of surveillance they are undertaking
- A list of common mistakes to avoid
- A suggested template form to be used when doing non-RIPA surveillance, not available elsewhere.

For more details:

[www.actnow.org.uk/content/26](http://www.actnow.org.uk/content/26)

You can also download an evaluation version. There is a substantial discount for those who bought earlier versions. ■

Code of Practice) Order 2010 will bring into force revised codes of practice on covert surveillance and CHIS.

The main changes to both codes are the same. The references below are to the Covert Surveillance and Property Interference Code of Practice (“the new code”) which covers directed surveillance, intrusive surveillance and property interference. Only the police and certain other agencies (not local authorities) have the power to do the latter two types of surveillance.

Directed surveillance (defined in section 26(2) of RIPA) is often conducted by local authorities to investigate a benefit fraud or to collect evidence of anti-social behaviour. It may involve covertly following people, covertly taking photographs of them, or using hidden cameras to record their movements. Section

28(2)(b) of RIPA states that an authorisation for directed surveillance should only be granted if it is proportionate to what is sought to be achieved by carrying it out. A regular criticism in OSC inspection reports is that public authority employees, when completing authorisation forms, do not give enough thought to proportionality and consequently authorisations are granted where the impact on the privacy of the target is disproportionate to the seriousness of the offence. Paragraph 3.6 states that the following elements of proportionality should be considered:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence
- explaining how and why the methods to be adopted will cause

Continued on page 11



Surveillance law and privacy

# Part 2 of RIPA... Continued from page 10

the least possible intrusion on the target and others

- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

Considering the examples in the code of surveillance activity which may not be proportionate (as well as speeches by Home Office ministers) it seems that the days of local authorities conducting directed surveillance for so called "minor offences" such as dog fouling and littering have gone. This may not be comfortable reading for many council officers who know that local taxpayers are often more concerned about these issues than so called "major crimes".

The new code considers it good practice for every public authority to appoint a Senior Responsible Officer (SRO). This should be someone of at least the rank of authorising officer, who is to be made responsible for:

- the integrity of the process in place within the public authority for the management of CHIS and directed surveillance;
- compliance with Part 2 of the Act

and with the Codes;

- engagement with the OSC inspectors when they conduct their inspections, where applicable



- where necessary, oversight of the implementation of post-inspection action plans approved by the relevant oversight Commissioner. Within local authorities, the SRO

should be a member of the corporate leadership team and should be responsible for ensuring that all authorising officers are of an appropriate standard.

For the first time, councillors in a local authority have been given a formal scrutiny role in relation to RIPA. The new codes states that, at least once a year, they should review the authority's use of RIPA and set the general surveillance policy. They should also consider internal reports on the use of RIPA at least on a quarterly basis to ensure that it is being used consistently as per the council's policy and that the policy remains fit for purpose. It is however emphasised that councillors should not be involved in making decisions on specific authorisations.

All public authorities need to raise awareness of the new RIPA provisions, especially among councillors and senior officers. Policies and procedures need to be revised and key staff will need to be trained ready for 6 April 2010.

### RIPA/RIPSA Update Workshops

Ibrahim Hasan and Sharon Heels will be discussing these changes in detail in our forthcoming RIPA Update/refresher workshops in Manchester, Edinburgh, Belfast and London. See

<http://tinyurl.com/yjmhjvt> ■

Surveillance law and privacy

## RIPA/RIPSA Helpline

Local authorities and other public sector organisations are increasingly doing complex

and time-consuming covert investigations to tackle benefit fraud, licensing issues and trading standards offences, anti-social behaviour and environmental health problems.

The Act Now RIPA/RIPSA Helpline is designed to supplement your internal surveillance law expertise by acting as a "sounding board" or "signpost service" for you to discuss your covert surveillance operations. Our experts will

guide you through the relevant area of law, discuss possible legal tactics and how to complete the relevant standard Home Office forms. The helpline will be managed by Ibrahim Hasan and Sharon Heels, who are renowned throughout the UK as the leading surveillance law experts.

Please click here for more information and subscription details:

[www.actnow.org.uk/content/25](http://www.actnow.org.uk/content/25) ■



## Surveillance law and privacy

# Surveillance news in brief

### RIPA conference

The Welsh Assembly government is planning a conference for RIPA authorities in Wales on the latest changes to the RIPA regime, which came into force on 6 April 2010. It will be on 21 April in Cardiff. Ibrahim Hasan will be speaking at this event. For more information please contact:

Adela Olah

Public Administration Division

Welsh Assembly Government

[email: adela.olah@wales.gsi.gov.uk](mailto:adela.olah@wales.gsi.gov.uk)

### RIPA update webcast

Ibrahim Hasan is doing a free web seminar on 13 April 2010 at 11am. He will examine the revised codes of practice under RIPA, which came into force on 6 April 2010. For more details and to register:

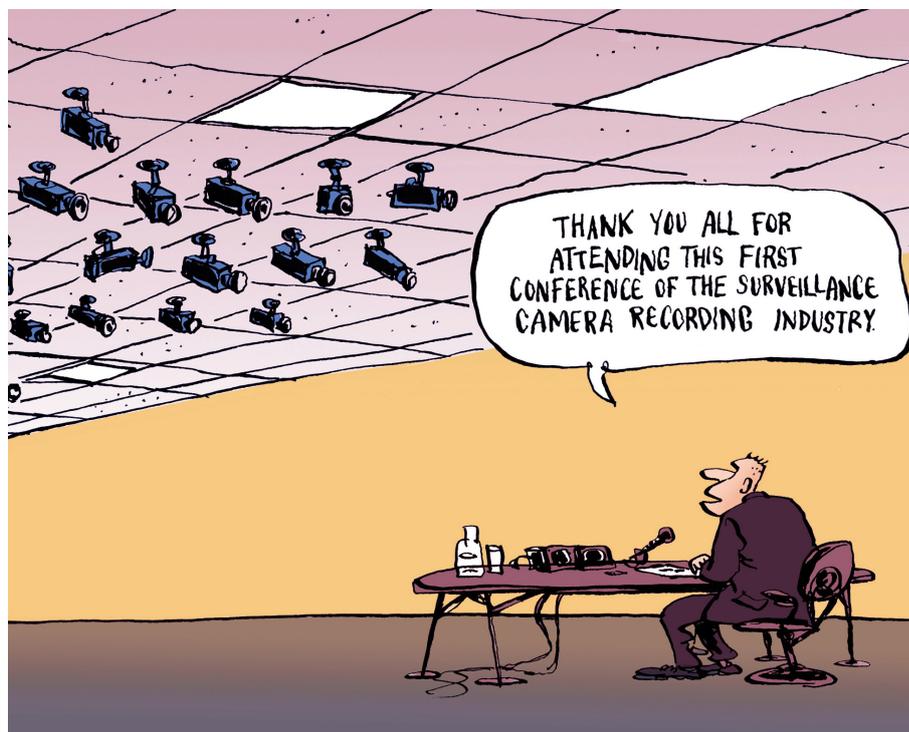
[www.actnow.org.uk/content/50](http://www.actnow.org.uk/content/50)

### Legal advice and consultancy

Our public sector experts can now assist you to practically implement FOI, DPA and records management. We can also give you legal advice in these areas. Why pay expensive lawyers and consultants who have little public sector experience?

For legal advice see Ibrahim Hasan's website:

[www.informationlaw.org.uk](http://www.informationlaw.org.uk)



Ibrahim can advise on all aspects of data protection, freedom of information and surveillance law. Recent instructions include appeals before the Information Tribunal and drafting and revising surveillance policies and procedures.

### In-house training

Act Now trainers also deliver in-house training at your site. In the last three months we have done in house training on FOI, EIR, DPA, data sharing and RIPA for:

- the Legal Services Commission

- General Medical Council
- London Borough of Redbridge
- Coventry City Council
- North Yorkshire Fire and Rescue
- North Tyneside Council
- Preston City Council
- Legal Services Commission
- Identity & Passport Service
- Mole Valley Council
- British Transport Police

If you would like a quote to bring the trainer to you please use our new online enquiry form:

[www.actnow.org.uk/content/12](http://www.actnow.org.uk/content/12)

## DISCLAIMER

The contents of this newsletter are meant for you to consider on the basis of general discussion and not as advice or expert opinion (legal or otherwise).

You are advised to obtain professional legal advice on specific issues. Any liability (in negligence or otherwise) arising from you acting or refraining from acting on any information contained in this newsletter is excluded.

### Copyright

This belongs to Act Now Training and we ask that anyone who wishes to subscribe does so via a form on our website. Your personal information will only be

used for the purposes of sending you this newsletter and information about our training course programme.

Public sector organisations can re-use material within their own organisation if they acknowledge our contribution by linking to [www.actnow.org.uk](http://www.actnow.org.uk)

**ACT NOW TRAINING LTD**  
**64 BRADFORD ROAD**  
**DEWSBURY WF13 2DU**  
**TEL 01924 451054**  
**FAX 01924 451129**