
UNITED KINGDOM NEWSLETTER

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

# BSI to adopt a new data protection standard

The British Standards Institution (BSI) invites comments on a new draft standard on the management of personal information, to be published in June, that will help compliance and develop best practice. **Laura Linkomies** reports.

This management systems standard aims to provide a framework that will enable an organisation to effectively manage personal information rather than prescribing exactly how operations should be run.

"The objective of this British Standard is to enable organisations to put in place a personal information management system (PIMS) which provides an infrastructure for maintaining and improving compliance with, amongst other things, the requirements of the Data Protection Act 1998 (DPA)," says the draft text that is now available for public comment until 31 March. Developed by a committee of experts including representatives from industry, government and academia, the standard will apply to any organisation which holds personal data.

> Consultation runs until 31 March.

According to the BSI, the standard is meant to be used by any size of organisation and should provide a common ground for the management of personal information.

A spokesman said: "Although BS 10012 is voluntary we believe that public and private-sector organisations recognise the importance of data protection and will be keen to implement the standard at the earliest opportunity. Data protection is an established area for BSI and we know that there is demand for products."

BSI states that it will be promoting BS 10012 and its benefits to relevant stakeholders via its usual communications routes: "The draft standard has wide support and potential users across industry and government, including backing from the Information Commissioner's Office."

## Personal Information Management System

The draft standard is centred on the idea of creating a personal information management system (PIMS) as part of the overall management system to establish, implement, operate, monitor, review, maintain and improve the management of personal information.

The standard would require organisations that agree to adopt the standard to develop, implement, maintain and continually improve their PIMS. Each organisation would define the scope of its PIMS and set personal information management objectives, with due regard to the:

a) requirements for the management of personal information;
b) organisational objectives and obligations;
c) an organisation's acceptable level of risk;

*Continued on p.3*

Issue 41 **FEBRUARY 2009**

## NEWS

UNITED KINGDOM
newsletter
ISSUE NO 41 February 2009

EDITORIAL DIRECTOR & PUBLISHER
Stewart H Dresner
stewart@privacylaws.com

EDITOR
Laura Linkomies
laura@privacylaws.com

DEPUTY EDITOR
James Michael
james.michael@privacylaws.com

NEWSLETTER SUBSCRIPTIONS
Glenn Daif-Burns
glenn@privacylaws.com

ISSUE 41 CONTRIBUTORS
Lucy Fisher
*PL&B* correspondent

Dugie Standeford
*PL&B* correspondent

Peter Church
Linklaters, London

PUBLISHED BY
Privacy Laws & Business,
2nd Floor, Monument House,
215 Marsh Road, Pinner,
Middlesex HA5 5NE, UK
Tel: +44 (0)20 8868 9200,
Fax: +44 (0)20 8868 5215
Website: www.privacylaws.com

The *Privacy Laws & Business* United Kingdom Newsletter is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of the newsletter. Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given. No part of this publication in whole or in part may be reproduced or transmitted in any form without the prior permission of the publishers.

Design by ProCreative +44 (0)20 8429 2400
Printed by Printflow Ltd +44 (0)20 7689 8697

ISSN 1472 9563



## comment

# New horizons for data protection

Justice Secretary Jack Straw has recommended Christopher Graham, Director General, Advertising Standards Agency (ASA), to become the new Information Commissioner. Meanwhile, Richard Thomas has outlined to the Commons Justice Select Committee (13 January) his views on ICO developments and changes to his role. Thomas, who will retire at the end of June, identified three major developments that have taken place under his six-year term:

- A modernised and confident ICO punching above its weight
- Freedom of information established as part of the fabric of public life
- Data protection taken seriously at last.

Unaware of Thomas's emphasis when planning this issue, we have reports that cover all three areas. Read on p.9 how the ICO is now pushing for senior executives to pledge a Personal Information Promise, and influences the way that ICO's new powers will be established in the Coroners and Justice Bill (p.4). On p.20 we discuss whether the FOIA is fulfilling its objectives after four years of being in force.

Much has been said about the interface between DP and FOI, but few are aware what is involved in an Information Tribunal hearing – something that is relevant both to DP and FOI managers. Read on p18. how to prepare for a hearing. On FOI disclosures, we alert you to the fact that your company information may not always be secure with the Financial Services Authority if there has been an informal settlement (p.19).

On the managerial side, this issue includes a substantial information package on how to obtain consent for marketing (p.12), and whether there is a need to acquire consent in the employment context (p.14). We also report on the draft data protection standard on which the British Standards Institution (BSI) is currently consulting (p.1). While this standard will be voluntary in nature, it will provide a new tool on how to measure and demonstrate best practice.

New technologies often pose DP challenges, and that is also the case in terms of "cloud computing". For example, if personal data is on a "cloud" outside of EU borders, rules on international data transfers need to be followed. For those who have been considering cloud computing, our report highlights the data protection and security concerns surrounding this technology (p.10).

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

### Contribute to PL&B publications

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on tel: +44 208 868 9200, or e-mail: laura@privacylaws.com.

*Continued from p.1*

d) statutory, regulatory and contractual duties; and
e) interests of its key stakeholders.

PIMS also requires organisations to publish a management policy that demonstrates support for, and commitment to, managing compliance with the DPA. The policy should include all elements included in the data protection principles and, in addition, organisations would commit to:

1. developing and implementing a PIMS to enable the personal information management policy to be implemented
2. where appropriate, identifying internal and external stakeholders and the degree to which these stakeholders are involved in the governance of the organisation's PIMS; and
3. the identification of individuals with specific responsibility and accountability for the PIMS.

Importantly, the policy requires making a member of the senior management team accountable for the management of personal information, and there is an expectation that the management of personal information should become a part of the organisation's core values. This would be ensured by, for example, raising, enhancing and maintain awareness of the PIMS through an ongoing education and awareness programme for all workers.

PIMS would also include inventories to identify high risk personal information such as sensitive data, risk management systems and regular audits. Internal audits and regular management reviews would assess the effectiveness and working of PIMS. As to how often these should be undertaken, that is a matter for each organisation, the BSI says. Much depends on the size and complexity of the organisation's operations.

And who should be made responsible for personal data? "The relevant person will vary between organisations according to where responsibility for data protection is positioned. The Information Commissioner's Office recommends that privacy should have board-level accountability," the BSI spokesperson said.

When asked about business views on the standard, the spokesman explained that the BSI's existing data protection products are popular across public and private sectors, and the BS 10012 drafting panel includes strong representation from the private sector, ensuring that the standard is relevant to business.

## Still time to put your views in

The draft standard also makes recommendations on how to provide notice, opt-out and online privacy statements.

It provides a useful list of definitions, for example about processing, which is described as obtaining, recording or holding personal information or carrying out any operation or set of operations on personal information. This includes collecting, organising, adapting, altering, disclosing, disseminating, aligning, combining, blocking, erasing and destroying personal information.

On the definition of "personal data", the draft guide refers to ICO guidance. Given the complex and ongoing debates and views by the ICO and the courts regarding the definition, this may be the best approach, even if not very user-friendly.

Gordon Wanless, Chairman of the DPC BS 10012 Drafting Panel and Chair of the Data Protection Forum, said: "This standard is the first of its kind in the area of data protection and is expected to be used widely by both public and private-sector organisations. Data protection has been the focus of much public attention over the last year and this standard will help organisations demonstrate that they are handling personal information responsibly. To ensure it is fit for purpose, it is extremely important that we receive comments on the draft standard, from both companies and individuals, and I would encourage anyone with an interest to express their views."

**INFORMATION**

The deadline for comments is 31 March 2009. The draft standard can be accessed and commented on at www.bsigroup.com/drafts (requires registration).
BSI has a number of publications that provide guidance on the processing of data (some of these will be updated on the publication of BS 10012):

- *BIP 0012 Data Protection Guide*
- *BIP 0050 Data Protection Pocket Guide – Essential Facts At Your Fingertips*
- *BIP 0011 Privacy in E-business – Promoting Respect, Trust and Confidence in your Organisation*
- *BIP 0002 Guidelines for the Use of Personal Data in System Testing*

## events diary

### PL&B EVENTS

**11 February 2009**
*Data Protection Training: Data Protection & Marketing Training, London*
This workshop focuses on the collection and use of personal information for direct marketing purposes.

**5 March 2009**
*Data Protection Training: Introduction to Data Protection, Leeds.*
This workshop is aimed at anyone who requires a basic course explaining the fundamentals of the Data Protection Act 1998.

**10 March 2009**
*Data Protection Training: Introduction to Data Protection, London*
This workshop is aimed at anyone who requires a basic course explaining the fundamentals of the Data Protection Act 1998.

**18 & 19 March 2009**
*DP Audit Training Workshops: Data Protection Auditing: Making the Information Commission's Audit Manual Work for you.*
This training is aimed at anyone who needs to conduct Data Protection Audits in their own organisation, or on companies processing your payroll or other data.

**6-8 July 2009**
PL&B's 22nd Annual International Conference, St John's College, Cambridge.
This conference provides an ideal opportunity for you to have direct contact with key decision makers at the world's leading international privacy event.

### OTHER EVENTS

**5 March 2009**
The Direct Marketing Association Data Protection Conference, London, UK.
Tel: 020 7291 3355, fax: 020 7323 4426, email: catherine.gibbon@dma.org.uk.

# Coroners and Justice Bill arms the ICO with new powers

The Coroners and Justice Bill seeks to introduce amendments to the Data Protection Act to strengthen the inspection powers of the Information Commissioner and to make data sharing easier if there is a strong public interest to do so (Part 8 of the Bill, published on 14 January).

On assessments, the Bill says that the ICO may require public-sector bodies to permit the ICO to enter premises, inspect documents, take copies of documents, observe processing of personal data and allow the ICO to interview persons who process personal data (*PL&B UK*, December 2008, p.1).

The ICO's commentary on the Bill, published before the Bill had its second reading on 26 January, says that it will also need the power to serve assessment notices on private-sector firms: "We have no desire to undertake heavy handed or widespread inspections. We only take action where we identify a specific risk to individuals, for example by analysing the tens of thousands of complaints that we receive each year – most of which are about private-sector organisations."

The ICO also demands a sanction where an organisation fails to comply with an assessment notice, and suggests an approach similar to s.54 of the Freedom of Information Act 2000, which treats failures by public authorities to comply with FOI notices as a contempt of court.

The ICO also calls for warrants for entry and inspection where there is reasonable suspicion that "there has been, or is likely to be" an infringement.

On information sharing, the ICO points out that the Bill's definition of "information sharing" is unclear: "As it stands, clause 152 says that a person shares information not only if the person discloses the information to another person, but also if the person consults or uses the information for a purpose other than the purpose for which the information was obtained. This legally convoluted definition will add to the considerable confusion surrounding information sharing. The ICO has to translate the law into simple, sensible guidance for organisations. This definition, which goes against the principle of clarity which lies at the heart of better regulation, will pose a considerable and avoidable obstacle. If the Government believes that there is need to address the use of information for a different purpose, then this should be done through a separate provision, not by stretching the meaning of 'sharing' beyond its normal usage."

The ICO welcomes the opportunity for a code of practice on data sharing. It says it can build on the ICO's current non-statutory code. However, the ICO points out that the Bill fails to make it compulsory for organisations with an information-sharing order to follow the code of practice.

The Bill was debated at Second Reading on 26 January 2009. The House of Commons voted for it to be sent to a Public Bill Committee that will scrutinise the Bill clause by clause. The committee consideration of the Bill will be finished on or before 5 March 2009.

• *The Coroners and Justice Bill is available at www.publications.parliament.uk/pa/cm200809/cmbills/009/09009.100-106.html and the ICO's commentary can be seen at www.ico.gov.uk/about_us/news_and_views/current_topics/cj_bill_commentary.aspx.*

# ICO takes enforcement action against the Home Office

The Information Commissioner's Office (ICO) has found the Home Office in breach of the Data Protection Act after a contractor, PA Consulting, lost an unencrypted memory stick holding sensitive personal details of thousands of individuals in August 2008.

The ICO has now required the Home Office to sign a formal Undertaking that will make the Home Office implement a number of security measures. With immediate effect, all portable and mobile devices which are used to store and transmit personal information must be encrypted. Any organisation processing personal information on behalf of the Home Office must also use encryption software, a requirement which must be clearly stated in all contracts. In addition, the Home Office will conduct regular inspections of the security of the data processor's facilities and carry out regular audits of the data processor's processing activities.

The Undertaking has been signed on behalf of the Home Office by Sir David Normington, the Permanent Secretary.

The ICO chose the route of an Undertaking rather than an Enforcement Notice as the Home Office launched an internal investigation immediately after the data breach and produced a report detailing action that had been taken or was planned for the future.

Mick Gorrill, Assistant Information Commissioner at the ICO, said: "We are investigating a number of the most serious reported data breaches. This case was serious because it involved thousands of individual records, which contained sensitive information on people serving custodial sentences and others previously convicted of criminal offences. This breach illustrates that even though a contractor lost the data, it is the data

controller (the Home Office) which is responsible for the security of the information. It is vital that sensitive personal information is handled properly and held securely at all times."

• *The Undertaking was published on 22 January and is at www.ico.gov.uk/upload/documents/library/data_protection/notices/home_office_undertaking.pdf.*

# Enforcement action against NHS Trusts

On 22 January The Information Commissioner's Office (ICO) found Abertawe Bro Morgannwg University NHS Trust and Tees, Esk and Wear Valleys NHS Foundation Trust in breach of the Data Protection Act.

Both NHS Trusts have been asked to sign formal Undertakings, which require the Trusts to implement a number of security measures to protect personal information more effectively. With immediate effect, all portable and mobile devices used to store and transmit personal data will be encrypted.

On 20 January, The Information Commissioner's Office required Hampshire Partnership NHS Trust and Southampton City PCT to sign formal Undertakings after finding the organisations in breach of the Data Protection Act 1998. The data breaches involved an incident which resulted in the loss of payslips containing employees' personal data from both trusts.

• *The Undertakings can be seen at www.ico.gov.uk/upload/documents/library/data_protection/notices/abm_swansea_undertaking.pdf. www.ico.gov.uk/upload/documents/library/data_protection/notices/tees_esk_and_wear_valleys_nhs_trust_undertaking.pdf. www.ico.gov.uk/upload/documents/library/data_protection/notices/hampshire_partnership_nhs_trust_undertaking.pdf. www.ico.gov.uk/upload/documents/library/data_protection/notices/southampton_city_pct_undertaking.pdf.*

# Consultation on privacy notices

The Information Commissioner's Office (ICO) has published a draft Privacy Notices Code of Practice, and is currently consulting on the content.

The ICO is of the view that often privacy policies are far too complex and contain too much legal jargon. The Code of Practice will help organisations to draft clear privacy notices and make sure that they collect information about people fairly and transparently. The Code contains good and bad examples that organisations will be able to use to help draw up their own privacy notices.

Deadline for comments is 3 April 2009. Please use a response form for submitting comments, available at www.ico.gov.uk.

# RIPA to be reviewed in 2009

The Home Secretary Jacqui Smith announced on 16 December 2008 that there will be consultation in early 2009 on the review of the Regulation of Investigatory Powers Act (RIPA). The purpose of the review is to examine

• a revision of the Codes of Practice that come under RIPA
• which public authorities can use RIPA powers
• how those powers are authorised, and who authorises their use.

Smith recognised the usefulness of RIPA, but said that there is a need to ensure the powers are used properly. She said that even with the clear safeguards that RIPA requires for the use of communications data and covert surveillance, she is "concerned at the level of misunderstanding there is about what these powers are, who has access to them, and what they can be used for".

Smith said that there have been cases where clearly these powers have not been used.

She is keen to find out whether the powers are authorised at a high enough level at local authorities. She suggested that perhaps the powers could be used only with the consent of a senior executive, and subject to a form of oversight from elected councillors.

# Lib Dems establish new privacy commission

Liberal Democrat Leader, Nick Clegg, announced on 13 January that the party has formed a privacy commission to tackle threats posed by extensive technology.

The Commission on Privacy will examine the use, abuse and retention of private data, and propose new safeguards to protect the rights of individuals.

The Commission's members are:

- David Heath MP (Chair) – Liberal Democrat Shadow Leader of the House
- Simon Davies – Privacy International; Fellow at LSE
- Shami Chakrabarti – Director of Liberty

- Baroness Sue Miller – Liberal Democrat Home Affairs Spokesperson in the House of Lords
- Henry Porter – Journalist on *The Observer*
- Prof. Ross Anderson – Professor of Security Engineering, University of Cambridge
- Richard Rampton QC – Barrister at law, specialising in libel
- Richard Allan – Former MP; Head of Government Affairs, Cisco Systems

Nick Clegg said: "With Britain now among the most watched upon countries in Europe, there has never been a more vital time for proper scrutiny and protection of privacy.

"Under this increasingly authoritarian Government, a combination of intrusion and incompetence has resulted in the steady erosion of our right to privacy and the protection of our personal data.

"This is an exceptionally well-qualified team bringing together experts from a wide range of fields. I am confident that they will work to provide real solutions to check the growing threat to our privacy."

# FSA warns shareholders of threat to personal data

The Financial Services Authority (FSA) has warned about 11,000 UK shareholders that their personal details are on a database shared by fraudsters, which can be used to target people and illegally sell them shares.

Share fraudsters are often based overseas and use high pressure sales techniques to target investors illegally, offering them non-tradable, overpriced or even non-existent shares.

The FSA wrote to the shareholders at the beginning of December 2008 after acquiring the fraud database with their personal details including names, telephone numbers and addresses, from Canadian authorities. It is likely that the list has been sold to a number of "share fraud" gangs.

# Education and Skills Act has DP implications

The Education and Skills Act, which received Royal Assent on 26 November 2008, raises the age level from 16 to 18 when young people can leave education or training. The new provisions mainly apply to young people who are resident in England, but some areas of the Act extend to Scotland and Wales, and there are DP implications in terms of sharing data on qualifications, benefits and employment. The participation age will be raised in two stages, to 17 from 2013 and to 18 from 2015.

- *The Act is available at www.opsi.gov.uk/acts/acts2008/ukpga_20080025_en_1.*

# Research group looks at consent

The EnCoRe project is studying how to make consent "as reliable and easy as turning on a tap, and revoking that consent as reliable and easy as turning it off again." The project links technology, process and regulatory research and development, and the project partners are:

- Hewlett-Packard Laboratories
- HW Communications
- QinetiQ
- London School of Economics
- Ethox Centre of the University of Oxford
- University of Warwick.

The project aims to enable business to adopt scalable, cost effective and robust consent and revocation methods for controlling the use, storing, locating and sharing of personal data. The first research findings are expected in spring 2009.

- Find out more at *www.encore-project.info/about.html.*

# New Guidance for local government on data handling

The Local Government Association and Society of Information and Technology Management (Socitm) have published new guidelines to improve data handling and processing within local government.

The guidelines, which were prepared by working closely with councils to meet local government circumstances, address DP challenges with regard to people, places, processes and procedures.

This includes awareness raising amongst staff, and emphasising that information is a key business asset and that its proper use is not simply an IT issue. All councils should ensure the security of their information through the physical security of their buildings, premises and systems. There should be regular assessments of information risks,

which are discussed by senior management. All councils should check that they have proper document systems in place and that their suppliers and contractors, when handling their information, work to the same standards. All councils should produce a Corporate Information Risk Policy which sets out how they will implement the measures proposed in this guidance, as well as produce policies for risk reporting and risk recovery.

The Guideline, published in November 2008, can be accessed at www.idea.gov.uk/idk/core/page.do?pageId=9040133 (or at www.socitm.gov.uk for Socitm members).

A £250,000 scheme to help councils implement the guidelines is being launched by the Improvement and Development Agency.

**Socitm's top 10 tips for data handling**

1. Ensure you understand which legislation affects your business area.
2. Ensure a named individual in the business, not ICT, owns the risk.
3. Ensure there is an effective incident reporting mechanism in place.
4. Regularly monitor, measure and audit your processes and procedures.
5. Establish a Corporate Information Governance group.
6. Ensure all staff are trained, updated and aware of their responsibilities.
7. Undertake regular risk reviews of all processes and procedures.
8. Ensure all key information assets are classified and are resilient.
9. Have robust risk driven processes in place for "ad hoc" situations.
10. Have documented policy driven processes and procedures in place.

# FFW launches BCR Club

The law firm Field Fisher Waterhouse (FFW) has launched a BCR Club for those working on Binding Corporate Rules ("BCR"). FFW's BCR Club is a forum comprising of in-house lawyers and privacy officers who are already working on a BCR project or are considering doing so.

The BCR Club will provide a forum for informal but in-depth discussion of legal and practical aspects of BCR, and an exchange of information amongst specialists.

The Club will have face to face meetings every quarter (including ad-hoc participation by representatives of data protection authorities), webminars for overseas members, ad-hoc emergency briefings, fortnightly e-mail updates and exclusive access to valuable BCR resources.

Membership is free but by invitation only.

• *For further information please contact Eduardo Ustaran, Partner, Field Fisher Waterhouse LLP, at eduardo.ustaran@ffw.com.*

# Ofsted must release names of child-care managers

The Information Commissioner's Office (ICO) has ordered the Office for Standards in Education (Ofsted) to release the names of 29,970 child care managers and their relevant place of employment in England following a request under the Freedom of Information Act.

Ofsted had released the following data as a response to the FOI requests: the name of each day care centre, the address, postcode, telephone number, the number of child day care places, the type of care each setting provides, the number of places for each type of care provided and the name of the owner (the provider). However, it had withheld the names of managers saying that it would breach the Data Protection Act.

The ICO says in its decision that there is a legitimate public interest, especially for parents, to get access to names of child care managers. The ICO notes that the names are already often in the public domain as there are directories available on the of day care centres, and many centres provide details of their staff on their own websites.

In addition, the information is held by Ofsted on a database from which the information can be downloaded. Ofsted initially denied holding information relevant to the request on the basis that collating the relevant material would constitute the creation of new information.

• *To see the full decision notice of 1 December 2008, go to web page www.ico.gov.uk/upload/documents/decisionnotices/2008/fs_50090869.pdf.*

# New advice on how to stop vexatious requests

The ICO has updated its guidance on how to deal with vexatious FOI requests, and says it will uphold public authorities' decisions to refuse requests where there is clear evidence that they are vexatious.

The Information Tribunal has backed the ICO's rulings to uphold public authorities' decisions in all ten appeal cases where a request has been turned down because it was deemed vexatious. The new guidance refers to these rulings when explaining how to judge whether a request is vexatious or not. If a request is vexatious, the public

authority should issue a formal refusal notice.

The guidance is available at www.ico.gov.uk/upload/documents/library/freedom_of_information/detailed_specialist_guides/awareness_guidance_22_vexatious_and_repeated_requests_final.pdf or telephone the ICO on 08456 306 060 to order a copy.

# Tribunal dismisses appeal regarding meta-request

The Information Tribunal has decided that the Information Commissioner (IC) was correct in finding that the public interest in maintaining the exemption in s.36 FOIA did not outweigh the public interest in disclosure of the information requested in a "meta-request".

Mr Davis of John Connor Press Associates had asked for information relating to the way 48 of his previous requests had been handled at the Home Office and the Ministry of Justice. Mr Davis requested an internal review which upheld the refusal notice. The IC found that the public interest in favour of maintaining the exemption did not outweigh the public interest in disclosure and ordered the disclosure of the information. The Home Office appealed to the Tribunal and the MoJ joined as an appellant.

The appellants claimed that exemption should be maintained, as:

1. There would be a chilling effect on the future conduct of those responsible for handling FOI requests;
2. There was a resources issue;
3. Meta-requests circumvented other processes provided for under FOIA for dealing with such matters;
4. The information contains little or no material of value;
5. Generally it is irresponsible to make meta-requests and they tend to serve private interests, and
6. They are a backdoor method of trying to obtain disclosure of exempt information.

However, the Tribunal found that "meta-requests" were not a special category of request under FOIA and that the IC did not err in law. The public interests in favour of maintaining the exemptions were largely of a general nature and that there was little evidence that they applied with any strength. The application of s.36 to a small part of the detailed information would need to be considered at a full hearing as insufficient evidence was available at the preliminary hearing.

• *The decision notice of 20 November 2008 is available at www.informationtribunal.gov.uk/DBFiles/Decision/i273/Home%20Office%20&%20MoJ%20v%20IC%20(EA-2008-0062)%20Decision%2020-11-08.pdf.*

# FOI requests with fictitious names can be refused

The Information Commissioner's Office (ICO) has published new guidance to help public authorities respond to information requests from people using pseudonyms or fictitious names to disguise their real identity.

According to the guidance, public authorities are entitled to treat a request as invalid, where the real name of the requester has not been used. The ICO itself will not be dealing with complaints that come from known pseudonyms and false names such as Mickey Mouse or Mrs Sue D. Nym.

The guidance urges public authorities to apply common sense. Where an obvious pseudonym is used, it is good practice for the public authority to consider the request as it may be happy to release the information, even though technically the request is invalid. If a public authority chooses not to comply with the request, then it should advise the applicant that the Freedom of Information Act requires their real name before the request is deemed valid.

• *The guidance is available at www.ico.gov.uk.*

# MPs' expenses to become public after all

MPs agreed, on 22 January, to reveal their expenses in more detail. The new publication system will introduce 26 separate categories, but it is not sure whether a full breakdown of MPs' spending will be made available. Harriet Harman, the leader of the Commons, said that MPs' expense receipts will be published back to 2004.

Further scrutiny is expected by the National Audit Office, which will check MPs' spending. Previously, MPs had to declare spending in just 13 categories.

The Government's decision to withdraw the proposed Order excluding MPs' expenses from the Freedom of Information Act was welcomed by the Campaign for Freedom of Information. Its director Maurice Frankel said: "We are delighted that this proposal has been shelved. It was wrong in principle for MPs to try and conceal their expenses claims when all other public servants have to release theirs. It was improper for the government to try and rush the measure through without the public noticing or having time to object. MPs should not be legislating on the quiet to remove an existing right of access to information about their own expenses in the hope that no-one will notice."

However, the Campaign suggested that it was possible that the measure would resurface in the near future in amended form. "Some MPs are clearly desperate to prevent the release of past expenses claims which are likely to have exceeded what could reasonably be justified to the public," Mr Frankel said.

# ICO helps increase accountability and supports privacy by design

The ICO is encouraging senior executives or board members to pledge a 'Personal Information Promise'. **Laura Linkomies** reports.

The ICO says that the Personal Information Promise has been designed, as a response to recent major data losses, for heads of organisations and government departments to demonstrate their organisation's senior level commitment to data protection. The aims of the initiative are to improve compliance with the Data Protection Act and help restore public trust and confidence. Executives can make the pledge by signing a standard letter that makes ten data protection promises (see separate box).

AstraZeneca's chief executive was one of the first to sign the pledge, witnessed by *Privacy Laws & Business* EPON participants.

The initiative, launched on 28 January, stems from an ICO-commissioned report "Privacy by Design", published in November 2008. As the ICO-designed 10-point pledge does not create additional legal obligations, it is more like a mission statement for privacy. The ICO does not intend to use the privacy promise as an additional regulatory tool, and says: 'we recognise that even with the best of intentions a problem can occur or there may be legitimately held views which differ from our own. It's the commitment to try to live up to the Promise that counts.'

The authors of the *Privacy by Design* report suggested that the "nominated defendant", in practice, a senior executive, would be expected to represent the organisation in a criminal or civil court if a data loss incident leads to a court hearing. The ICO has not specified anything like this idea. So will the Promise have any effect?

Yes, in terms of alerting the senior levels at your organisations to privacy issues, and demonstrating privacy-friendliness to customers. However, in terms of nailing organisations down to improve compliance, the promise is unlikely to deliver, as signatories are likely to be organisations that already take data protection seriously.

## Challenges with privacy by design

Other aspects in the "Privacy by Design" report by the Enterprise Privacy Group, published on 26 November 2008 (*PL&B UK*, October 2008, p.19), include support for the use of Privacy Enhancing technologies (PETs), and Privacy Impact Assessments (PIAs). In practice, this means making sure that privacy concerns are addressed at the beginning when designing new systems, rather than trying to bolt them on afterwards. PIAs can indeed be useful in identifying the need for PETs, and should be started right at the design phase of a new project.

However, the report identifies several barriers to privacy design. It is often the case that senior managers do not recognise their responsibility to protect privacy, or simply want to address privacy purely as a data protection compliance issue. Also, organisations often fail to recognise that there are privacy requirements throughout the project's lifecycle. Even if PETs are available, they have not been widely adopted, partly because good research has not always been turned into commercial products. Also, organisations and vendors are hesitant to commit to specific PETs as they can quickly become obsolete. And on top of everything, there is a jungle of privacy and data protection concepts, and people are sometimes talking about issues with the wrong names.

## ICO action

While work has been done on standards, there is a need to develop a common practical standard, the ICO says. However, any standard should have an international status, and the ICO says it will take part in global discussions.

Organisations may, in the future, have a chance to tell the ICO when registering what type of privacy enhancing projects they have completed, for example, a PIA. The ICO will revise its PIA handbook in early 2009, and will do more to help explain key data protection concepts, for example, the difference between identification and authentication.

## What else can be done?

The report identifies several areas where improvements could be made. It recommends working with industry bodies to build an executive mandate for privacy by design. This could include preparing sample business cases which would illustrate the costs, benefits and risks associated with data processing. Alongside with encouraging a wider use of PIAs, the authors say that standards for cross-sector data sharing are needed.

To further improve accountability, authors suggest that organisations could be made to declare an asset and liability value for personal data within their end of year accounts. One of the problems is that the public sector does not value personal data as an asset. The drivers for ensuring information security are much stronger than protecting privacy.

The authors also stress that there is a pressing need for the development of a professional body for privacy practitioners. The ICO says it will consider the need for such a body, which could train, accredit and promote the work of data protection professionals.

The British Computer Society (BCS) is currently drafting a personal data guardianship code. It also proposes that the existing DP principles should be amended to include consent of data

subjects for data sharing, and the right to revoke consent. It also wants to see sound data governance principles and the right to limit access. In the case of data sharing, the original data collector should retain stewardship of data. By stewardship, the BCS means that the collector of data has the duty to look after it throughout the information life cycle.

## Conclusion

The Information Commissioner, Richard Thomas, said that much greater awareness is needed about privacy issues. However, he recognised that we have already moved away from privacy being a minority interest, and the terms often used now are "leadership" and "governance". Board-level commitment is needed, though, to make a real difference, he said.

Organisations that have already signed the pledge:

- Action for Children
- Acxiom
- Astra Zeneca
- Belfast City Council
- British Gas
- BT
- Callcredit Limited
- Dudley Primary Care Trust
- Experian
- Equifax
- Field Fisher Waterhouse
- Greater Manchester Police
- Informing Healthcare
- Isle of Anglesey County Council
- NHS Information Centre
- Northern Ireland Association of Citizens Advice Bureaux
- Royal Mail
- T-Mobile
- Unison
- Vodafone

### PERSONAL INFORMATION PROMISE

**I** (name and title),
**on behalf of** (name of organisation)
**promise that we will**:

1. value the personal information entrusted to us and make sure we respect that trust;
2. go further than just the letter of the law when it comes to handling personal information, and adopt good practice standards;
3. consider and address the privacy risks first when we are planning to use or hold personal information in new ways, such as when introducing new systems;
4. be open with individuals about how we use their information and who we give it to;
5. make it easy for individuals to access and correct their personal information;
6. keep personal information to the minimum necessary and delete it when we no longer need it;
7. have effective safeguards in place to make sure personal information is kept securely and does not fall into the wrong hands;
8. provide training to staff who handle personal information and treat it as a disciplinary matter if they misuse or don't look after personal information properly;
9. put appropriate financial and human resources into looking after personal information to make sure we can live up to our promises; and
10. regularly check that we are living up to our promises and report on how we are doing.

**Signed**
(name and title)
**Date**

# Cloud computing: How risky is it really?

**Lucy Fisher** tries to unpick a privacy challenge.

In the current economic climate, what could be better than shedding your business of the burden of large, unwieldy servers, data sets and software packages and leaving that for someone or something else to deal with, more cheaply? In theory, this is what happens in the world of "cloud computing". The concept is not new, but it is in recent months that the term has become a buzzword in the world of corporate IT.

The idea is that computing services are divorced from your hardware and shifted to a server, or servers, on the worldwide web. This means that your data can be available from anywhere, on a plethora of different devices. Companies like Microsoft, Google, Amazon and Apple are all competing for cloud custom, delivering information and software over the internet, in the "clouds".

The advantages of such scalable, pay-as-you go type services, are in no doubt – they are often cheaper, as well as "greener", and they can take the hassle out of managing large servers. But the issues surrounding privacy and security are far less clear. In fact, the term "cloud computing" has been subject to lively debate in recent months and is the source of considerable controversy.

Larry Ellison, founder of software giant Oracle, lambasted the notion publicly as "fashion-driven". His views are echoed by Martyn Thomas, visiting Professor of Software Engineering at the Oxford University Computing Laboratory and a fellow of the Royal Academy of Engineering: "People go charging off after new ideas, and they aren't yet good at the basics. The data processing will be outside your control, in who knows what jurisdictions. I'd expect the Information Commissioner to ask very serious questions," he says.

## Cloud poses data transfer issues

Whilst growing awareness and ensuing polemic surrounding the "cloud" has increased – along with offerings such as

Google's Gmail and GoogleApps, and Apple's MobileMe – the use of such services for casual purposes, such as uploading personal photos or organising your own calendar, are unlikely to pose a problem. It is when commercial organisations, processing large amounts of personal data, take to the cloud that problems may arise. So, before your company invests in the clouds, what privacy and security concerns do you need to consider?

The issue of jurisdiction is key. The clouds are, by definition, global, so your data may be subject to a patchwork of legal and regulatory requirements depending on where it is at any one time.

Dan Cooper, partner at law firm Covington & Burling says that it is crucial, before you sign an agreement with any provider, to ask where your data will be held. "Work out where the clouds are," he says. "If they are outside the EU, you'll need to find a solution to the issue of international data transfer."

It may well suit the service provider not to specify where data is being held, but if the customer is based in a jurisdiction with restrictions on what can be done with personal data, then this may not be good enough and should not necessarily be accepted. "Some cloud computing companies are far more sophisticated than others," warns Christopher Millard, a consultant at law firm Bristows, Professor of Privacy and Information Law at Queen Mary University of London and Senior Research Fellow at the Oxford Internet Institute.

Where data is being exported from is also key, since, even within Europe, the rules can vary from country to country with regards to the assessment of the 'adequacy' of the privacy protection provided for particular transfers of data. As Millard points out, it may be easier for UK-based controllers to ensure adequacy: "The UK has a pragmatic, DIY-style adequacy test based on a risk assessment which may permit transfers without any formalities and it also adopts an informal approach to the use of EU-approved standard contract clauses. The style elsewhere in the EU tends to be more bureaucratic, with many regulators insisting on filings or approvals for data exports. Fortunately some destinations, such as Switzerland, are on a 'white list' that all EU Member States must respect."

And finding the right solution to the international transfer issue poses another series of conundrums, as Renzo Marchini, a solicitor at Dechert explains: "Model contracts are applicable when your data is somewhere, not anywhere; Safe Harbor applies only when the recipient is in the United States and there's no further traffic; and BCRs apply only to group companies."

## Third party concerns

Despite all the grey areas, what is certain is that you will need to demonstrate the due diligence required by the Data Protection Act. So, when putting your data in the hands of a third party you need to make sure that your chosen provider is reputable. And, as with any data flow in your business, there must be a high degree of transparency for processing to be deemed fair in the eyes of EU data protection law. If the terms and conditions seem vague as to who will have access to the data, how long it will be held, when it may be destroyed and what kind of security will be provided, you are taking a big risk.

Although it may be harder to make demands of cheaper, commoditised services, this is unlikely to be a valid excuse for any negligence – despite experts, such as Ross Anderson, Professor of Security Engineering at Cambridge University, claiming that some providers are highly unlikely to have customer service at the top of the agenda. "The typical business can no more negotiate with Google than a typical patient negotiate with the NHS. You take it or leave it. You can't even get to talk to anyone knowledgeable," he warns.

Another place to start in assessing risk is to look at who is likely to be responsible for losses that might occur in the cloud. According to the Data Protection Act, it is the controller of the data who must make sure that the processor takes all necessary steps to treat data lawfully – and that is most likely to be the company that chooses to outsource, even if it is paying someone else to handle certain functions.

But once again, life is not always that simple. According to Marchini, it can be a moot point in some instances who is the controller and who is the processor: "There is guidance, supposedly in the pipeline, from the European Union's Article 29 Data Protection Working Party on this matter," he says. In any case, given that most regulators hold the user of the service ultimately responsible for the security of their data, any cloud computing provider that will not submit to external audits and security certifications, is holding up a red flag.

Here, another word of warning. According to Professor Thomas: "I haven't checked the disclaimers, but I'd guess that the cloud computing companies do not insure you for loss – especially the consequential damage to your business if anything does go wrong. And how is the service protected? Could it be hacked? Most websites can be penetrated if you are willing to put in enough effort."

There is a political dimension, too. "It's an issue for regulators if lots of information about Europeans is being held outside of Europe," adds Cooper.

Indeed, when data is being stored on servers in another jurisdiction, you may be exposed to inspection by local regulators – which in turn, could lead to publication of all sorts of material despite confidentiality, trade secrets or data protection laws – and potentially without your permission or prior knowledge. The United States, for example, permits broad US-style discovery in aid of non-US proceedings when information is stored in other countries.

With such fears in mind, some of the more forward-thinking companies are devising solutions to common problems. Millard predicts that some of the larger providers may start to offer European-only based cloud services, within the next year to eighteen months.

"There is a business opportunity for service providers to take the initiative and provide EU privacy-friendly cloud computing services, whereby there's a guarantee that your data will not leave the EU or an approved country. In this way you could regionalise the cloud for customers who do care about where

*Continued on p.23*

# Back to basics: Obtaining consent for marketing

Gaining consent for unsolicited direct marketing messages can mean negotiating a maze of laws, regulations and codes of practice. Careful planning of marketing objectives – and asking the right questions – can help, DP practitioners say. By **Dugie Standeford**.

Consent "is a minefield," said Les Kingstone, group data protection officer for Aegon UK, an insurance conglomerate. Organisations must navigate the law, ICO regulations, and, for some, industry self-regulatory codes such as the Advertising Standards Authority's Code of Advertising, Sales Promotion and Direct Marketing. Aegon tries to be the "whitest of the white" by adhering to the ASA code, whose provisions are stronger than legal requirements, he said.

Section 11 of the Data Protection Act (DPA) 1998 covers all direct marketing, defined as "the communication (by whatever means) of any advertising of marketing material which is directed to particular individuals." Companies that process personal data for direct marketing must comply with both the DPA and, if they use electronic marketing channels, the Privacy and Electronic Communications (EC Directive) Regulations (PECR) 2004.

The PECR defines electronic mail as email and text, picture and video messages, the ICO said in an 8 October 2007 electronic communications guidance document. Moreover, "we consider that this rule also applies to voicemail and answerphone messages left by marketers making marketing calls that would otherwise be 'live,'" it said. The rules do not cover "silent calls" via fax or other electronic signal, which do not involve transmission of marketing material.

Under the DPA, processing of any personal data requires consent by the data subject. The PECR additionally requires consent to unsolicited electronic mail marketing, the ICO said: "You cannot transmit, or instigate the transmission of, unsolicited marketing material by electronic mail to an individual subscriber unless they have previously notified you, the sender, that they consent, for the time being, to receiving such communications."

The regulations provide for a "soft opt-in" exception, however, that allows unsolicited e-marketing to individual subscribers without prior consent where:

- The marketer has obtained the recipient's contact details in the course of a sale or negotiations for the sale of a product or service to the recipient;
- the direct marketing material being sent relates to the sender's similar products and services only; and
- the recipient has been given a simple way to refuse, (free of charge except for the cost of transmission) the use of his or her contact details for marketing purposes at the time those details were initially collected and, where they did not refuse the use of those details, at the time of each subsequent communication.

The ICO provides guidance on interpreting key terms such as "similar products and services" and "in the course of a sale or negotiations for the sale of a product or service."

Unsolicited telephone marketing calls and faxes to individuals are governed by the Telephone Preference Service and Fax Preference Service, respectively, suppression registers operated by the Direct Marketing Association on behalf of the Office of Communications. The association also runs a Corporate Telephone Preference Service for business subscribers. The Mailing Preference Service, also funded by the direct marketing industry, allows consumers to remove their names from sales mail lists.

## Obtaining consent

All companies carrying out unsolicited direct marketing are bound by the rules but they interpret them to suit their individual circumstances, said Opt-4 Director Jenny Moseley, whose consultancy helps marketers "conduct permission based marketing that complies with" the DPA and PECR. There is a tendency to over-comply by, for example, using opt-in consent when soft opt-in is appropriate. Companies uncertain about the rules often "go over the top" – and discover they are stifling their own data collection, she said.

The ICO PECR direct marketing compliance checklist provides a template for determining whether, and what kind of, consent is needed.

Moseley and Kingstone stressed that consent must be obtained at the first point of contact in a marketing relationship. The seller should offer a data collection notice that covers the required channels to market (paper, email, telephone and so forth), and states whether the company will use the data itself and/or share it with outside third parties, said Moseley. No matter what the marketing route is, data protection notices may cover other channels as well, she said: A direct mail coupon will not only collect permissions for postal communications but also for other channels that may be important to the organisation, such as email.

Retrospective permission is difficult to obtain because many people fail to respond to such requests, leaving their feelings about receiving unsolicited marketing materials unclear, said Kingstone. Requiring someone to opt-in to sales pitches may be difficult, he said, but a marketer who has obtained such consent knows he has a firm lead.

Aegon generally deals directly with independent financial advisers (IFAs) who then interact with individual consumers seeking insurance, Kingstone said. Sales consultants make contacts in IFA offices whose opt-in consent they

obtain before marketing new products to them. Although the PECR does not apply to companies, Aegon complies with it anyway in its transactions with IFAs, making its consent process stricter than either the DPA or PECR, he said.

Consumer opt-out consent to receive future communications from Aegon is sought via a tick-box at the back of the application form at the time a potential policy-holder's request for insurance is made. Policies come with a two-page fair processing notice which also tells policy-holders how to avoid future marketing solicitations. However, Aegon is not very active in the direct-to-consumer market, generally contacting them directly only for purposes related to their policies, Kingstone said.

Tick-boxes on printed and electronic coupons or registration screens are one way to enable individuals to refuse unsolicited marketing materials, Moseley said. Other options include:

- Emailing to a specific address, in other words delete@xxxcompany
- Writing to an address provided
- Calling a specified telephone number
- Going to a "my preferences" page online (email account).

The company, not the person wishing to change his or her preferences, should bear all costs, Moseley said. A freephone number or freepost address should be provided.

## Is 'soft opt-in' appropriate?

Marketers who want to use electronic means should ask themselves several questions, Moseley said.

1. Is this a consumer transaction? Soft opt-in does not apply to business dealings.
2. Am I a charity? Collecting permission to seek donations must be by opt-in as the ICO does not consider them sales.
3. Is this sensitive data? If so, opt-in must be used.
4. Am I looking to collect third-party permission for email contact? Then consent must be by opt-in.
5. Is my offer for similar services and products? If so, soft opt-in can be used.
6. Do I intend to collect data and permissions as part of a negotiation for a sale? Soft opt-in applies here.

Organisations may use soft opt-in even when it is not required, but "this may be over-compliant and may reduce the number of contacts" they gather with permission, she said.

## To bundle or not?

"Bundling" a data subject's consent for use in different marketing channels and for third-party contacts uses less space on a coupon but may not be completely compliant if third-party email or text permission is sought by opt-out, said Moseley.

Bundling gives the consumer less choice, she said. The response that "I'd be happy for you to send me e-mails but I don't want phone calls" may lead to less "permissioned" data for the organisation. Listing all the permissions in one block with separate tick-boxes takes up more room; and if there are opt-outs and opt-ins mixed up together with multiple tick-boxes, the person may tick all or none. Moseley said she prefers a hybrid version. A hybrid version is where in certain circumstances for certain companies, some efforts to gain permission are grouped together and some are separated by the most important channel to the company. For example, if email is the most important channel for a company, the manager will make best efforts to obtain email addresses and permission before other channels.

## Compliance headaches

UK direct marketers face many challenges in complying with consent rules, said Moseley.

Key among these are knowing how to interpret the legislation, applying it to the circumstances of their own business, and keeping up to date with changes in its interpretation, she said. Organisations also need written policies and procedures which they control internally and with third parties outside the company, including contractual terms for data security rules.

She recommended that marketers keep track of upward or downward trends in permissions according to media channel and put test plans in place to correct or capitalise on the level of consents acquired. In addition, companies should write their data collection notices so they comply with the law, are on-brand, match their stated policies and procedures, and are honest and open to encourage consumers to give permission for future contacts, she said.

In explaining the meaning of "on-brand" Mosely tied the writing of data collection notices to brand values. Copywriting data collection notices so that they are compliant with the legislation, should be "on brand," in that they match the company's stated policies and procedures, and are transparent and honest so that the consumer will be more encouraged to give their permission for future contact.

**INFORMATION**

1. Guidance for marketers on the Privacy and Electronic Communications (EC Directive) Regulations 2003: www.ico.gov.uk/upload/documents/library/privacy_and_electronic/detailed_specialist_guides/guidance_part_1_for_marketers_v3.1_081007.pdf.
2. Data Protection Good Practice Note, Charities and marketing: www.ico.gov.uk/upload/documents/library/data_protection/practical_application/charities_and_marketing_12_06.pdf.
3. Data Protection Good Practice Note, Electronic mail marketing: www.ico.gov.uk/upload/documents/library/data_protection/practical_application/electronic_mail_marketing_12_06.pdf.
4. PECR Direct Marketing Compliance Checklist, Template: www.ico.gov.uk/upload/documents/pia_handbook_html/files/PECR%20checklist.doc.
5. PECR Legal Obligations: www.ico.gov.uk/what_we_cover/privacy_and_electronic_communications/your_legal_obligations.aspx.
6. Good Practice Note, Calling Customers on the TPS: www.ico.gov.uk/upload/documents/library/data_protection/practical_application/calling_existing_customers_on_the_tps.pdf.
7. Advertising Standards Authority, British Code of Advertising, Sales Promotion and Direct Marketing: www.asa.org.uk/asa/codes/cap_code/CodeIndex.htm?code_id=21#expanded.
8. The Direct Marketing Association, Code of Practice: www.dma.org.uk/Membership/mem-Code.asp.
9. www.dma.org.uk/_attachments/Resources/45_S4.pdf.
10. *New Data Protection Liabilities & Risk for Direct Marketers – practical aids to legal and successful permission marketing*, by Jenny Moseley and Rosemary Smith.

"On brand" means that you might write a different data collection statement for a young audience than you would for an over 50's audience. Therefore, where a company has a number of brands or communication strands, creative writing should be adapted to an individual brand audience. But the meaning of the words should match the overall policies on data collection.

People are the main challenge, said Kingstone. Processes and procedures may be correct but humans sometimes don't think, he said. Moseley recommended regular staff training. An organisation should also monitor what happens within its marketing materials to "see if anyone is unwittingly causing a problem," she added.

### Recommendations

Rule number one for businesses starting out in direct marketing is to think carefully about what their objectives are in collecting the data, both said. That includes why they are gathering it and from whom, what they plan to do with it, how they will store it securely, and whether they will transmit it outside the European Economic Area, Moseley said. "Prevention is better than cure."

"Don't restrict yourself to the current technologies you're using," Kingstone said. Aegon's recent revamp of its database, for instance, has prompted a debate on whether to use faxing as a contact channel, he said.

Kingstone's final advice: "Best of luck."

**AUTHOR**

Dugie Standeford is a PL&B correspondent.

# Back to basics: obtaining consent from employees

**Laura Linkomies** looks at the difficulties of acquiring consent at the workplace, and how to stay within the law.

One can argue that it is impossible to obtain a "freely given" consent in an employment relationship – and this is the view of the EU's Art. 29 Data Protection Working Party (consisting of all 27 national Data Protection Authorities). However, employers need to seek employees' consent when they cannot rely on other legitimate grounds for processing personal data.

To make things more difficult, the UK Data Protection Act has no specific definition of consent, and hence the ICO advises that "The Commissioner's view is that consent is not particularly easy to achieve and that data controllers should consider other conditions … before looking at consent.'

The ICO has also said, in relation to international data transfers, that "Consent must be freely given…but consent is unlikely to be valid if the data subject has no real choice but to give his/her consent … consent must also be specific and informed. The data subject must know and have understood what he/she is agreeing to."

### Recruitment

Employers need to seek consent during the recruitment process. To ensure compliance with the Data Protection Act, application forms should warn the employee about the employer's intention to process his/her personal data and ask the applicant for his/her consent. When the individual is recruited, many organisations seek to obtain blanket consent in the employment contract.

HBOS Data Protection Manager Sue Taylor explains: "HBOS will capture consent for processing for recruitment activity on the application form. If the individual is employed, at their induction they are provided with a copy of the HBOS data protection guidance on employee data that details how the company will process their information and their rights under the DPA."

If the employees then wish to withdraw their consent, there are two different scenarios. "Employees can withdraw consent to marketing at any time.

However, other processing is essential for the maintenance of their records and the employment relationship with that individual. Therefore, we would not necessarily rely on consent to process. There may be a legal obligation to process or we may rely on the "legitimate business interest" schedule 2 condition for processing," Taylor explains.

A representative from the financial services sector, company A, says that withdrawing consent depends on what the consent relates to. Much of the processing that takes place relates to their obligation to meet the terms of the contract (for example payroll, provision of benefits, etc.) or fulfil our legal obligations (for example Financial Services Authority rules, crime prevention and Health & Safety). If the employee chose to withdraw their consent to the former example then it is likely that the relationship between the two parties would cease. For the latter example, consent is not required so this is not relevant.

Company A tries to acquire blanket consent at the start of employment. The company has a full but understandable privacy statement in the staff handbook and a more detailed Employee Data Policy, which further explains to staff how their information may be used. However, in many cases, one can rely on the legitimate interests ground.

When it comes to leaving the company, organisations should not provide confidential references about a worker unless asked to do so by the individual in question. At HBOS, the HR department, that manages all business areas, will provide a reference only if the appropriate consent has been supplied by the requestor.

Company A said: "Our employee

data policy informs employees that unless they instruct otherwise, we will provide employment references on ex-employees, if requested. Such references contain very limited information, for example confirmation that they worked here and the duration of employment. For all other references, because they require more detailed information, we would require the specific consent of the employee before releasing any information."

## Disclosing information

Employers are often asked employees' information by other organisations, and need to take extra care in protecting employee data. There may be legitimate grounds for the disclosure, for example a legal obligation stated in other laws relating to, for example, criminal investigations. The ICO says that where possible, organisations should seek and take account of the workers' views.

Susan Taylor says that at HBOS, requests for employee information normally come from one of the following;

- The employee themselves using their right of access
- Government organisations such as HMRC
- Trade Unions
- Third parties acting on behalf of an employee (such as a solicitor)
- Financial Crime prevention organisations.

Taylor explains that no information is provided unless they have a legal obligation to provide it or the consent of the individual. The only exception may be for financial crime prevention where they may decide to rely on voluntary disclosure under S29. However, each request is reviewed on its own merits.

Company A says that the requests they receive fall into the following categories:

- HMRC/DWP – Statutory requests are always fulfilled and the organisation would consider voluntary requests on a case by case basis
- Court Orders – need to comply
- Police – Statutory requests are always fulfilled and would consider voluntary requests on a case by case basis
- Employment references – these requests are received from various parties. Will comply with these requests upon receipt of the employees' consent
- Mortgage /Rent reference – Due to the level of information requested, will only respond to these upon evidence of the consent of our employee
- Job Centres – We rarely respond to these as they do not include employee consent
- Solicitors – We will only respond upon evidence of consent from the employee.

## Using data for marketing

Employers should not release personal information for marketing purposes, unless they have acquired employees' consent for this use. When new employees join the organisation, you need to inform them if your organisation plans to use their details for sending them marketing messages. Employees are entitled to not give their consent.

The ICO's advice is to take the following action:

- Review whether your business markets its, or anyone else's, products or services to current or former workers.
- Ensure that any new worker who will receive marketing information from your company has been informed that this will happen.
- Ensure that a clear procedure for "opting-out" is made known to all workers.
- Do not disclose workers' details to other organisations for their marketing unless individual workers have opted in.
- Review whether your business discloses workers' details. If so, put in place a procedure to ensure that a worker's details are not passed on until you have received a positive indication of agreement from him or her.

If planning to market to existing workers for the first time either in ways that were not explained when they first joined or that they would not expect, you need to obtain their consent. The ICO says it is acceptable to include this type of marketing in a mailing that they receive anyway, for example a pay-slip, as long as the offer tells employees how to opt-out.

"HBOS does not allow employee information to be used by third parties for marketing unless they have given their explicit consent. This is normally only in relation to arrangements we have with third parties for discounted products," Taylor says. "HBOS employees can write to our payroll department to opt out of any HBOS direct marketing."

The DP manager from company A says: "The privacy statement in our staff handbook informs employees that we may market them and this includes the option to opt out of any such communication. Employees can register their opt-out online or by post."

## Publishing employee information

The ICO advises that if you decide to publish information about employees, e.g. in an annual report or on the company website, you need to consider whether you need employees' consent to do so. Make sure that the information is not harmful to them. Ensure that the employees know what information will be published, where and for what purpose. Organisations should take extra care when publishing employee data on the Internet.

Company A says that they would only ever publish employee information with the prior consent of their employees as in most cases, this would be unexpected. For more senior staff (e.g. board members), this would be a regular occurrence but this is an expected part of their role and as such they would have implied consent.

HBOS does not publish employee information on their external websites unless they have the consent of the individual. Employees used within their marketing material volunteer for their information/image to be used for that purpose.

## Monitoring

Company A tells us that their Acceptable Use Policy clearly states that there are occasions where their individual email accounts may be monitored, including when they are absent. This policy forms part of their terms of use of email and is made available to all employees. Consent is implied when they accept the policy by using their systems.

Employers do have legitimate reasons for some monitoring but this should be restricted to certain areas and

employees should always be informed of monitoring and the reasons for it, unless investigating an offence. The ICO says that employers who can justify monitoring on the basis of an impact assessment will not generally need the consent of individual workers.

Emails can be opened without employees' consent but this should be avoided wherever possible, especially if it is possible to establish which are private ones. If you need to check someone's e-mail when they are away from the workplace, make sure that you inform that individual.

### Health

An employer must not approach an employee's GP for a medical report without first obtaining the employee's written consent. There are limitations as to how far consent can be relied on as a basis for the processing of information about workers' health. The ICO says that for consent to be valid, it must be:

- Explicit. This means the worker must have been told clearly what personal data are involved and have been properly informed about the use that will be made of it. The worker must have given a positive indication of agreement, for example a signature.
- Freely given. This means the worker must have a real choice whether or not to consent and there must be no penalty imposed for refusing to give consent.

Employers should collect health information only where this is necessary for the protection of health and safety, to prevent discrimination on the grounds of disability, to satisfy other legal obligations or if each worker affected has given his or her explicit consent. Blanket consent obtained at the outset of employment cannot always be relied on.

Company A says that explicit consent to process sensitive information such as health data is sought at the beginning of employment as this is the only time that it can be "freely given". This in the privacy statement (which refers to sensitive information) and forms part of the employment contract. However, health data is collected in very limited circumstances.

### Consent is a tricky issue

Clearly obtaining consent is a tricky issue. When asked what are the most challenging aspects of trying to acquire employees' consent, the DP managers had the following to say:

"HBOS tries not to rely on consent in an employment context as it appreciates that in many circumstances, consent cannot be freely given. If we were unable to obtain or rely on consent we would always look to develop a process or activity that could be legitimately processed under another condition for processing."

"One of the trickiest areas relates to financial crime prevention and/or whistleblowing activities where there many be an element of covert data processing taking place. Our processes reflect the need to assess each matter on its own merits before any action is taken".

Company A's data protection manager says: "It really is questionable as to whether employee consent is ever freely given. Even upon commencement of employment, the individual really wants the job so is not normally in a position to negotiate the terms of the use of their data. Also, even though consent can be withdrawn at any time, it is difficult to see how the employer/ employee relationship could continue if the employee withdrew consent or objected to the processing of their information.

On this basis, it is always sensible to rely on a different condition for processing employee information, for example performance of contract, legal requirement and legitimate interest of the data controller."

# European Court rules that DNA storage violates privacy right

The European Court of Human Rights in Strasbourg on 5 December 2008 ruled unanimously that the United Kingdom violated the right to privacy, reports **James Michael**.

A Grand Chamber of 17 judges of the European Court of Human Rights in Strasbourg on 5 December 2008 ruled unanimously that the United Kingdom violated the right to privacy by taking and storing indefinitely the DNA and fingerprints of people who had not been convicted of any offence. In the two cases of *S. and Marper v. the United Kingdom*, the Court decided that that the finding of a violation, with the necessary consequences for the future, was enough, and did not award any financial compensation. It did award €39,387 for financial expenses. Because the judgment was made by the Grand Chamber, there can be no further appeal.

One applicant had been arrested when he was eleven and charged with attempted robbery. His fingerprints and DNA samples were taken and stored, although he was acquitted. Mr Marper was arrested and charged with harassment of his partner. His fingerprints and DNA samples were taken and stored, although the case was formally discontinued. Both unsuccessfully requested that their fingerprints, DNA samples and profiles be destroyed. The law authorised the retention of the data for an unlimited time.

The Court accepted that the retention of fingerprint and DNA information was for a legitimate purpose, namely the detection, and therefore, prevention of crime. It noted that fingerprints, DNA profiles and cellular samples constituted personal data within the meaning of the Council of Europe Data Protection Convention of 1981. The issue, said the Court, was whether the retention of the fingerprint and DNA data of the applicants, as persons who had been suspected, but

not convicted, of criminal offences, was necessary in a democratic society. The Court ruled that it was not.

The court noted that most of the Council of Europe states allowed such materials to be taken in criminal proceedings only from individuals suspected of having committed offences of a certain minimum gravity. In the great majority of the states with functioning DNA databases, samples and DNA profiles derived from those samples were required to be removed or destroyed either immediately or within a certain limited time after acquittal or discharge. A restricted number of exceptions to this principle were allowed by some states.

The Court noted that England, Wales and Northern Ireland appeared to be the only jurisdictions within the Council of Europe to allow the indefinite retention of fingerprint and DNA material of any person of any age suspected of any recordable offence.

It observed that the protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests. The Court was struck by the blanket and indiscriminate nature of the power of retention in England and Wales. In particular, the data in question could be retained irrespective of the nature or gravity of the offence with which the individual was originally suspected or of the age of the suspected offender; the retention was not time-limited; and there existed only limited possibilities for an acquitted individual to have the data removed from the nationwide database or to have the materials destroyed.

The Court expressed a particular concern at the risk of stigmatisation, stemming from the fact that persons in the position of the applicants, who had not been convicted of any offence and were entitled to the presumption of innocence, were treated in the same way as convicted persons. It was true that the retention of the applicants' private data could not be equated with the voicing of suspicions. Nonetheless, their perception that they were not being treated as innocent was heightened by the fact that their data were retained indefinitely in the same way as the data of convicted persons, while the data of those who had never been suspected of an offence were required to be destroyed.

The Court further considered that the retention of unconvicted persons' data could be especially harmful in the case of minors such as the first applicant, given their special situation and the importance of their development and integration in society. It considered that particular attention had to be paid to the protection of juveniles from any detriment that could result from the retention by the authorities of their private data following acquittals of a criminal offence.

### Blanket retention failed to strike a fair balance

In conclusion, the Court found that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, failed to strike a fair balance between the competing public and private interests, and that the respondent State had overstepped any acceptable "margin of appreciation" in this regard. Accordingly, the retention in question constituted a disproportionate interference with the applicants' right to respect for private life and could not be regarded as necessary in a democratic society. The Court concluded unanimously that there had been a violation of Article 8 in this case.

### UK ACTION

The ruling will have a major impact on how UK police force operates. However, the Court did not specify how the UK should achieve compliance. In a statement, Home Secretary Jacqui Smith said: "DNA and fingerprinting is vital to the fight against crime, providing the police with more than 3,500 matches a month, and I am disappointed by the European Court of Human Rights' decision."

On 16 December 2008, in a speech to Intellect, a trade association for IT professionals, Smith announced that the government will immediately begin to remove the DNA of children under 10 from the database.

Smith said: 'We will consult on bringing greater flexibility and fairness into the system by stepping down some individuals over time – a differentiated approach, possibly based on age, or on risk, or on the nature of the offences involved."

"That may mean letting the 12 year old… come off the database once they reach adulthood. And it could mean limiting how long the profiles of those who have been arrested but not convicted of an offence could be retained."

"We are also re-examining retention arrangements for samples. Physical samples of hair and saliva swabs that represent people's actual DNA are much more sensitive than the DNA profile that is kept on the database – which only uses a small part of non-coding DNA."

Smith said that a forensics White Paper will be published in 2009, and it will include proposals for consultation on the retention of DNA data.

# Putting your case to the Information Tribunal

Putting your case to the Information Tribunal can be daunting but careful preparation will help you present yourself most effectively. **Stewart Dresner** reports on how Jan Turner, Staffordshire Police's Information Compliance Officer, dealt with a Tribunal case.

The case before the Information Tribunal in 8-18 April last year was an appeal by her Chief Constable and those of Humberside, Northumbria, West Midlands, and Greater Manchester against the Information Commissioner's Enforcement Notices delivered in August and November 2007.

The case involved five sample cases which turned on whether each of the police forces should have retained or deleted records on the five individuals from five to 30 years after the minor offences took place. In the case of Staffordshire, the case involved a 13 year old girl who had been violent against an older girl and had received a reprimand. Now the attacker was 18, she wanted to seek work in child care and had had no offences since the incident. She had been told that the record would be removed by the time she reached 18 if she stayed out of trouble. There had been no further incidents but the record had not been deleted. The Information Commissioner's case was that the record should be removed from the Police National Computer to enable her to find a job in her chosen field.

While this Tribunal case focussed on these five cases, everyone was aware that they represented many more similar cases involving the 43 police authorities across the UK. This was a precedent for the Information Commissioner, the five police forces, their colleagues in the rest of the UK and the Association of Chief Police Officers whose successive codes on the retention of personal data on the Police National Computer were highly relevant to this case.

As Jan Turner has responsibilities which include compliance with the Data Protection Act, the Freedom of Information Act and records management, she appeared as a witness before the Tribunal to support her Chief Constable.

This Tribunal was chaired by the Chairman himself, Professor John Angel and two non-legal Members, Richard Fox and Nigel Watson. The five Chief Constables were represented by barrister David N. Jones and the Information Commissioner were represented by another barrister, Timothy Pitt-Payne.

The official report of the case (at www.informationtribunal.gov.uk/DBFiles/Decision/i200/Chief_Constables_v_IC_final_decision_2007081_web_entry[1].pdf) runs to 48 pages and gives the Tribunal's decision in considerable detail.

Reading the report gives very useful insights into the process as well as the basis of the decision. It is clear that the Tribunal pays great attention to the statement of each witness, who are all named with their professional roles. Their statements are analysed and compared with the statements of other witnesses to show how the Tribunal reaches its decision. While a Tribunal is designed to be less intimidating than an appearance in a court, and a hearing can take place in any suitable premises anywhere in the country, a Tribunal hearing has a distinct formality. There is undoubtedly a judicial atmosphere enhanced by the fact that each side is likely to be represented by a barrister. Also, both sides know that the Tribunal's decision may lead one of them to appeal to the Court of Appeal, if the losing side considers it sufficiently important. There the Tribunal's decision will be carefully reviewed and attention may focus on any of the witness statements, for example, for accuracy and consistency.

## Preparation before giving evidence

As Jan Turner was fully aware of the importance of the case for her chief constable, she took the following steps before giving evidence which represents her advice to anyone appearing before the Tribunal:

1. Prepare as much as you can
2. Liaise with colleagues involved in the case and ensure that you are familiar with the process and the policy issues relating to your case – in this case, retention policy, the "step down" procedure (for holding but not releasing certain data an issue at the heart of this case), and the police force's internal procedures for dealing with requests to "step down" or "step out" (delete) personal data
3. Carry out a full independent review of the facts and interpretations specific to your case to ensure that you have considered the requirements of the Data Protection Act and any other relevant law, such as the Freedom of Information Act
4. Make contact with someone who has previously given evidence at the Tribunal to discuss the process
5. If possible, go and sit in at another Tribunal hearing, as you will learn a great deal from this experience.

## Advice for giving evidence

Jan gives this advice based on her experience of participating in the Tribunal hearing:

1. although you will often be asked questions by a barrister or other legal representative, remember to direct your responses to the Panel of Tribunal Chair and non-legal members. There is a natural tendency to address a response to the person asking you a question. But in this case, it is the Panel which

is conducting the hearing and therefore, you must literally direct your attention to them.
2. speak clearly which not only clarifies communication but also gives you an opportunity to present your case in a credible style.
3. don't be afraid to ask for a question to be repeated
4. if you don't understand a point, say so, don't try to bluff your way through
5. stay calm and bear in mind that there is no need to panic – after all, this is a process to determine the law on a specific point in which the Tribunal aims to understand from each witness the detailed rationale for their position.

Finally, says Jan, remember to treat the other side as fellow data protection professionals and speak to them in a normal friendly manner. You have usually dealt with the Information Commissioner's staff in the past to discuss various issues, and will no doubt do so again. The Tribunal hearing is one moment in time where you are both trying to resolve how the law should be interpreted. You need to argue your case to the best of your ability before the Tribunal but ensure that you retain goodwill for the future.

### The Tribunal's decision

The Tribunal published its decision on 21 July 2008 in favour of the Information Commissioner in all five cases. But the Police Service has lodged an appeal which is now scheduled to be heard at the Court of Appeal on 22-24 June.

• *Stewart Dresner, Editorial Director, reported on Jan Turner's presentation to the Annual Conference of the National Association of Data Protection and Freedom of Information Officers on 19 November 2008.*

# Is your information safe with the FSA?

**Peter Church** explains why information about informal FSA settlements may not be protected.

Financial services firms have become relatively comfortable that information they provide to the FSA will not be disclosed under the Freedom of Information Act 2000. This is because the FSA is subject to a statutory prohibition on disclosure of information it receives in the course of its duties.

However, a recent decision by the Information Tribunal tests the limits of this prohibition and found that information about informal settlements may not be protected as it is not "received" by the FSA. The decision is subject to appeal but, in the meantime, is relevant to any firm considering an informal settlement with the FSA.

### The Lautro 19

The Tribunal's judgment relates to two requests for information to the FSA. The first asked for the names of the firms who used inappropriate charges when providing endowment mortgages, the so-called Lautro 19. The second is for the names of firms who were subject to a mystery shopping exercise. This article concentrates on the former request.

The use of inappropriate charges was a serious issue. Inappropriate charges have been applied to over 600,000 policies and the firms agreed to pay compensation estimated to be £274 million. However, because the firms had paid compensation voluntarily, the FSA did not censure them or take any other enforcement action. The FSA's view was that a firm that "cooperates with this approach does not expect to be the subject of the formal sanction of publicity". Moreover, "disclosure of the names of companies now would potentially undermine the willingness of those companies, and regulated companies in general, to engage in open dialogue with it".

Such arguments did not impress the Information Commissioner who decided that the names of the firms were not exempt and must be disclosed. The FSA appealed against that decision to the Tribunal.

### Preliminary issues: Statutory bar on disclosure

The request potentially engages a number of exemptions, including that disclosure would prejudice the FSA's law enforcement activities and would prejudice the commercial interests of the Lautro 19. However, the Information Tribunal decided to deal with a single exemption as a preliminary issue – whether disclosure of the names of the Lautro 19 is prohibited by or under an enactment (section 44 FOIA). The relevant statutory provisions are:

- section 348 of the Financial Services & Markets Act 2000 ("FSMA"), which prohibits the FSA from disclosing information received for the purposes of its functions; and
- sections 205-207 of FSMA, which prevents the FSA publicly censuring a firm without following certain statutory procedures.

### Section 348: Did the FSA 'receive' the information?

The FSA received a wide range of information from the Lautro 19 as part of their investigation and, on the basis of that information, the FSA concluded that those firms had applied inappropriate charges. The issue was whether disclosure of the firms' names is an implicit disclosure of the information collected earlier in the process.

In deciding this issue, the Information Tribunal referred to *Melton Medes v SIB* [1995] CH 137. In relation to the predecessor to section 348, Lightman J decided that "Disclosure of what is a mere possible deduction from information is not as it seems to me, at least in this context, disclosure of the information itself". Applying such reasoning, the disclosure of the firms' names would not result in the disclosure of any information received by the FSA as

it is not "possible to effect a trail back to the confidential information which was in issue". In particular, disclosure of this information would not enable anyone to discover the nature of the inappropriate charges, the period during which they were used or any other information received as part of the investigation.

As an alternative, the FSA argued that releasing the firms' names would disclose some form of agreement between the firms and the FSA to compromise the dispute. However, the Tribunal dismissed the suggestion that any such agreement could constitute information "received" from the firms in question (following similar reasoning to the Tribunal's decision in Derry City Council v Information Commissioner).

### Sections 205-207: Disclosing firm name a public censure?

The FSA has the power to publicly censure a firm under section 205, subject to a number of safeguards including an obligation to serve a warning notice, to give the relevant firm a right to state their case and a right to appeal to the Financial Services and Markets Tribunal.

The FSA argued that disclosing the names of the Lautro 19 would be a finding that those firms had used inappropriate charges and had been held liable to compensate customers. It would therefore amount to issuing a public censure without applying the necessary safeguards and due process. The Tribunal had little time for this argument, finding that the relevant prohibitions in FSMA did not constitute a prohibition on disclosure and, even if they did, they were not applicable to disclosures under FOIA.

The Tribunal was also dismissive of the suggestion that the disclosure would be an infringement of the firms' right to a fair trial and right to privacy under Articles 6 and 8 of the European Convention on Human Rights. The firms' settlement with the FSA was a voluntary choice on their part and they did not reserve their rights under Article 6 or 8. Moreover, Article 8 does not constitute a statutory prohibition on disclosure for the purposes of FOIA.

### Appeal to the High Court

The FSA has already lodged an appeal at the High Court challenging the Tribunal's interpretation of section 348 and sections 205-207. This is unsurprising as the decision could have a serious impact on the FSA's ability to reach informal settlements with firms in the future. Moreover, if the Tribunal's interpretation is incorrect and the FSA does release the information, then the FSA risks committing an offence.

If the appeal is unsuccessful then the Tribunal will have to consider if the information is exempt for other reasons, for example because disclosure would prejudice its law enforcement activities or would prejudice the commercial interests of the Lautro 19. Therefore, it may still be some time before the firms' identities are uncovered.

The Information Tribunal's judgment in Financial Services Authority v Information Commissioner EA/2007/0093 and 0100 is available from the Information Tribunal's website, www.informationtribunal.gov.uk.

**AUTHOR**

Peter Church is an associate in the Technology, Media and Telecommunications group at Linklaters LLP, London.
Email peter.church@linklaters.com

# Is the Freedom of Information Act meeting its objectives?

Eight years after adoption of the Freedom of Information Act in 2000 and four years after its entry into force, University College London's Constitution Unit is conducting research to assess whether this law is meeting its objectives. **Stewart Dresner** reports.

The campaign for a Freedom of Information law in the UK for more than 20 years drew on experience in the US, Canada and several other countries. While traditional access methods continue, such as MPs' Parliamentary Questions and millions of calls a year to call centres run by central government, government agencies and local government departments, campaigners and advocates expected several specific benefits from the UK having this FOI law.

Drawing on materials from several countries for this research project, the Constitution Unit has identified six main objectives of an open government law as follows:

1. Transparency: Is government more transparent and is there more proactive disclosure?
2. Accountability: Is anyone interested in an issue more able to make government agencies more accountable by asking typically both what happened and who is to blame?
3. Better decision-making process: Has FOI improved decision-making – is it more open, does it stick to process, is there a better information flow?
4. Public understanding of decision-making: Is anyone interested better able to understand who and why decisions are made?
5. Participation in the political process: Is there a discernible increased participation in the political process?
6. Trust: Does the public have increased trust and confidence – is government more impartial, listening more, and more responsive?

The Constitution Unit is using the following research methods:

- Interviews providing case studies from eight government departments
- An online survey of requesters

resulting in 130 responses and interviews with selected requesters and stakeholders
- An ongoing analysis of more than 1,000 articles and a sample of the FOI related Parliamentary Questions in the 2005 to 2008 period
- A review of decisions taken by the Information Commissioner and the Information Tribunal.

### 1. Transparency/openness

There is a consensus among requesters, public authorities and the media that FOI has indeed increased transparency and proactive disclosure, for example, related to government ministers' expenses and meetings. Evidence includes over 650 articles which used the FOIA to obtain information about a story on central government in the 2005-2007 period. Of these, 9% give a "new insight" into a subject, predominately historical records or issues relating to health, social policy and defence.

### 2. Accountability

The researchers refer to both "narrative accountability" (what happens?) and "culpable accountability" (who is to blame?). The results of the study suggests that FOI "slightly sharpens" accountability. Examples are MPs being made accountable for how they spend their allowances; what happened and who was to blame for reform of the tax dividends on pensions; Greenpeace used the FOI to hold the Department for Business, Enterprise & Regulatory Reform to account for its decision on its nuclear power consultation which helped lead to a judicial review and a new consultation. However, according to some opinions, audit, media and judicial review has a far stronger impact on culpable accountability. One person said: "The accountability that matters was always there and is still there." But 56% of the media articles use the FOIA to make the government accountable in some way. Parliamentary questions (PQs) are still to be analysed but even at this stage it is clear that they are less often about MPs' use of the FOIA and more about the law itself.

### 3. Better quality of government decision-making

This point was explained by then Lord Chancellor, Lord Falconer in 2004: "The more there is a culture of openness, the better decision-making will be. If decisions have to be publicly explained, they will be better taken." In theory, a better decision is more open and based on a clearer information flow. However, in practice, the survey results are that the FOIA has not made decision-making any better. Any improvements to decision-making have been brought about by other factors, for example, the Better Regulation Initiative and the government's commitment to consultation.

Opinions differ over whether the FOIA has led to a "chilling effect" where decisions are taken by telephone or meetings which are not recorded, or recorded in a sanitised or less informative way, and circulated to fewer people. A typical comment is: "Does [FOI] mean that we keep lots of things off paper? Well, we always did." In short, the consensus from the interviews is that FOI has not had much of an impact.

> The FOIA has not made decision-making any better.

### 4. Public understanding of decision-making

"Freedom of information… is about giving people the chance to understand how Government works and why it has reached particular decisions" declared Lord Chancellor, Lord Irvine in 1997. In short, does FOI help the public to understand how and why a decision is made? For example, Greenpeace obtained e-mails between Minister, John Hutton and energy company E. on over whether to include a controversial storage system in a bid for a coal-powered power station in Kent it was subsequently removed.

Of the media articles, 17% gave an insight into decision-making. Overall, the results show that public understanding is slightly increased by the FOIA. The survey of requesters and media both show some increase in public understanding due to FOI of how and why decisions are made.

### 5. Public participation

"Without openness we cannot hope to encourage greater participation in our democratic life" said Lord Falconer in 2004. In short, does FOI promote political engagement? The researchers give two examples of how the FOIA may have led to an increase of public participation in the political process:

Firstly, Greenpeace's use of the FOIA regarding the nuclear power consultation led to a new consultation process. Secondly, regarding the expansion of Heathrow Airport, opinions differ on whether publicity generated by the FOIA "exposing collusion" between government and suppliers increased the number of people participating in protests.

Opinions among those interviewed in government departments differ partly depending on whether the interviewee regarded FOI itself as a form of participation. Among this group, few thought that FOI fostered wider political engagement.

However, the picture is different from the perspective of requesters. More requesters did something "participative" with the information than did not. The most common uses of the information were for:

1. Research
2. Submitting another FOI request.
3. Using the information to voice a disagreement with a policy and/or sharing the information with a campaign.
4. Seeking more information without using the FOIA.
5. Due to these conflicting views, there is no consensus on whether the FOIA increases participation in the political process.
6. Trust.

Tony Blair said in 1996 that the introduction of FOI "will signal a new relationship between government and people… given on trust". Therefore, the researchers' key questions in this category were:

1. Does FOI increase trust and confidence in government?
2. Does FOI affect perceptions of key indicators, in particular, the government's impartiality, ability to listen, and responsiveness?

For example, more information has been published on MPs' expenses, and the media and public see how some MPs are spending their allowances. However, trust in politicians continues to fall. The problem may stem from the context within which government and the media operate. The conflicting relationship of "spin" and negative reporting combine to undermine or reverse the intended effect of FOI. Disclosure then reinforces negative perceptions, rather than bringing leading to the development of more positive views. Moreover, public trust rises or falls according to a complex interplay of factors, of which openness is only one.

This ambiguity demonstrates that trust is a complex issue. One interviewee said: "paradoxically, at least to start with, trust in the government might well go down as… public coverage produced tends to be about government failure."

The researchers' conclusion on trust is that FOI has not increased trust in government. The analysis of the media and the requester survey both indicate a neutral or harmful effect on trust, and the interviews produce ambiguous results.

**INFORMATION**

This report is based on a presentation by the researchers, Ben Worthy and Mark Glover, at the Constitution Unit, headed by Professor Robert Hazell, on 19th November 2008. These results are provisional, as the research will continue until the end of June 2009.
Further information is at www.ucl.ac.uk/constitution-unit/foidp/events/2008/ImpactofFOI.htm.

# Is the Government recriminalising the leaking of official information?

Director of the Campaign for Freedom of Information, Maurice Frankel, wrote to *The Times* on 4 December 2008 pointing out that the Damian Green case (in which a civil servant allegedly leaked information to this Conservative MP) raises the question of whether the offence of misconduct in public office is now being used as a way of recriminalising the leaking of official information.

Frankel wrote: "For many years any leak of official information on any subject – damaging or innocuous – was an offence under Section 2 of the 1911 Official Secrets Act. The 1989 Official Secrets Act changed this. It limited the offence to unauthorised and damaging disclosures relating to the work of the security and intelligence services, defence, international relations and law enforcement or to the obtaining of information under certain warrants, for example to intercept communications.

"The 1988 White Paper that announced the reform made clear that disclosures that were merely 'undesirable, a betrayal of trust or an embarrassment to the Government' would not be punishable by the criminal law. Introducing the new legislation Douglas Hurd, then the Conservative Home Secretary, explained that it 'will remove the protection of the criminal law from the great bulk of sensitive and important information – including policy documents, Cabinet discussions on education, on health and on social security, and economic information and budget preparations. None of them will any longer have the protection of the criminal law'. Such disclosures might lead to disciplinary action – but not prosecution.

"The disclosures that the Home Office civil servant are alleged to have made not only fall within the broad class of information deliberately removed from these criminal sanctions but in some cases are likely to be disclosable under the Freedom of Information Act. How has the clock been turned back to make such disclosures the subject of police investigations, arrests and possible prosecutions?"

# book reviews

**Laura Linkomies** reviews *The privacy advocates: Resisting the spread of surveillance*, by Professor Colin J. Bennett.

Apart from being a highly entertaining read for privacy anoraks who personally know many of the actors behind these privacy movements, the book provides an interesting insight into privacy battles, who they are fought by, why, and where. Most importantly, the book reveals that privacy advocates are becoming more powerful and have indeed managed to successfully challenge and overturn some of the most intrusive surveillance practices. Bennett studies these groups in order to explain how they can be distinguished from others in the privacy circuit, and looks at whether it is likely that the groups will form a social movement or a

transnational activist network.

Bennett notes that the groups, mostly to be found in the US, where the lack of omnibus federal privacy legislation encourages a variety of different groups, are highly influential. They are very good at organising online campaigns, petitions, electronic newsletters etc to aid their cause. Even if they do not have many resources, there have been some real successes, for example, the campaigns against Google, Intel and Microsoft. One of the most successful international campaigns ever was against DoubleClick in 1999-2002. The issue was about DoubleClick's ability to positively identify people browsing on the internet and send them targeted advertising. An appeal to shareholders and other measures saw DoubleClick share price drop 20 per cent. According to Bennett this was largely due to privacy concerns. Another good example is Microsoft passport that lead to an investigation by the EU Data Protection Commissioners.

In Europe, privacy advocacy is not quite as common, partly due to people seeing the Privacy Commissioners as spokesmen for the issues. Privacy International, based in London but with an international presence, has engaged in most privacy issue over the years. In the UK, NO2ID campaigns against ID cards, and there are other small, one issue campaigns.

Despite great visibility, good contacts and an organised nature, Bennett is unsure whether we are experiencing a new social movement. Perhaps it will be in the future, as privacy advocacy is still a very elitist issue where most actors are specialists in legal, technical, policy or organisational fields. We can, however, talk about a loose transnational advocacy network, as there is increasing co-operation between actors.

It is these observations and the evidence of privacy advocates having successfully fought some of the world's largest companies that make the book an essential read for anyone who wants to understand the changing nature of the international privacy scene, or wishes to prepare for some unwanted attention.

**INFORMATION**

Colin J. Bennett is Professor in the Department of Political Science at the University of Victoria, British Columbia, Canada.
*The privacy advocates: Resisting the spread of surveillance*, published in October 2008, ISBN 978-0-262-02638-3, £18.95

*Continued from p.11*

their data is located," he explains.

This is likely to help in many instances but may come with a price tag. And it goes without saying that, before committing to any cloud computing practices, you will need an effective governance structure, to know and understand data flows within your business.

Then, if you do decide to go ahead, as well as asking who will be processing the data, and how, find out whether there will there be any subcontracting. Any company using cloud computing services should look at setting up standard agreements on the handling of personal data.

## Cost savings at a risk

Certainly the services may appear cheaper but without the necessary due diligence at the outset – and before you sign on the dotted line – it could work out as a costly risk to your business in the long run. Anderson explains: "Breaches will probably be fewer, but bigger. This is a common pattern with technology. The invention of power grids made power cuts rarer but ensured they would affect millions of people when they did happen."

Research firm Gartner, in a report entitled *Assessing the security risk of cloud computing*, published last June, advises companies to demand transparency. "Don't contract for IT services with a vendor that refuses to provide detailed information on its security and continuity management programs," it says.

For secure transmission, you will need some encryption, especially for sensitive data. And providers should have an easily available security policy and privacy policy in addition to their terms of use. Amazon Web Services and Salesforce.com, for example, include these policies on their websites.

But encryption of sensitive data is the bare minimum you should do. Recognising this, Accenture is currently working on a research programme around the area of data anonymisation – whereby, with any given piece of data, characteristics which are important for an application are preserved, while aspects of the data that are not relevant are masked. Kishore Swaminathan, Accenture's chief scientist, explains that, in terms of precautions that can be taken when cloud computing, data anonymisation could be used alongside the obvious encryption technologies for greater security.

In any case, a cloud provider should include provisions protecting you against data intrusion by their staff with physical access to the machines. According to Omer Trajman, director of field engineering at Vertica Systems: "Since many cloud infrastructure providers use virtualised hardware and your machine may be reassigned if it has a critical failure, your Service Level Agreement should include provisions on automatic data wiping for any shared resources."

*The Economist*'s technology correspondent, Ludwig Siegele, says that regulation of the cloud is needed before large companies, on any large-scale start using it. "Will Google or Microsoft, for example, do it?" he asks. "If that doesn't happen, I think Governments will step in. Perhaps a better solution is that technology firms anticipate and build a system where they have borders."

For the technology to be as advantageous as it could be, users must demand safeguards. As things stand, despite the apparent advantages of cloud computing, the question still remains as to whether it will be technology or the law that takes necessary steps to ensure it is fully compliant.

**AUTHOR**

Lucy Fisher is a PL&B correspondent.

# Your Newsletter Subscription **Includes**

**1. Six newsletters a year**
The *Privacy Laws & Business (PL&B) United Kingdom Newsletter*'s scope ranges beyond the Data Protection Act to include the new Freedom of Information Act, related aspects of the Human Rights Act and the Regulation of Investigatory Powers Act. It also covers Jersey, Guernsey and the Isle of Man. The newsletter complements the *International Newsletter*, which has been the leading data protection and privacy publication for 21 years.

**2. Email updates**
We will keep you frequently informed of the latest privacy developments.

**3. Country, Subject, Company Index**
Subscribers will receive annually a cumulative subject index of all topics covered. Multiple headings include advertising, data security, Internet, police, transborder data flows and sensitive data. The index is updated after every issue on our website www.privacylaws.com.

# e-Newsletter

**Electronic Option**
The newsletter is available, for an additional enterprise licence fee, in PDF format for uploading onto your intranet or network. This format enables you to see the newsletter on any computer on your network as it appears in the paper version. It allows you to print out pages at any location. Please contact the *Privacy Laws & Business* office for more information.

*Privacy Laws & Business has clients in over 45 countries, including the UK Top Ten, eight of the Global Top Ten and seven of Europe's Top Ten in the* Financial Times *lists; and 10 of the US Top 20 in the* Fortune *list; and 70% of the top 20 law firms in the London and UK Legal 500 lists.*

# Newsletter Subscription Form

## *Subscription Packages*

(Please add 15% VAT to prices for the PDF format within the EU)

❑ **Print** ❑ **PDF** (please tick preferred delivery format)

❑ Send a FREE sample of the *UK/International Newsletter*

❑ *PL&B UK* Subscription **£285**

❑ *UK/International Newsletter* Combined Subscription **£595** or an extra **£220** for existing International newsletter subscribers

❑ Special academic rate – 50% discount on above prices

**Multiple Subscription Discounts**

❑ 2-9 copies: 30% discount (indicate no. of copies .....)

**Intranet Enterprise Licence (inc. up to 10 printed copies)**

❑ *PL&B UK* **£1,425**

❑ *PL&B International* **£1,875**

❑ Both *International/UK Newsletters* **£2,975**

❑ I wish to receive *PL&B's* FREE e-mail news service

**Data Protection Notice:** *Privacy Laws & Business* will not pass on your details to third parties. We would like to occasionally send you information on data protection law services. Please indicate if you *do not* wish to contacted by: ❑ Post ❑ Email ❑ Telephone

Name:

Position:

Organisation:

Address:

Postcode: Country:

Tel:

Email:

Signature:

Date:

## *Payment Options*

Address of Accounts (if different):

Postcode:

❑ Purchase Order

❑ Cheque payable to: *Privacy Laws & Business*

❑ Bank transfer direct to our account:
*Privacy Laws & Business*, Barclays Bank PLC,
355 Station Road, Harrow, Middlesex HA1 2AN, UK.
Bank sort code: 20-37-16 Account No.: 20240664
IBAN: GB92 BARC 2037 1620 2406 64 SWIFTBIC: BARCGB22
*Please send a copy of the transfer order with this form.*

❑ American Express ❑ MasterCard ❑ Visa

Card Name:

Credit Card Number:

Expiry Date:

Signature: Date:

***I am interested in:***

❑ Consultancy/Audits
❑ In-House Presentations/Training
❑ Recruitment Service

*Please return to:* Newsletter Subscriptions Department,
Privacy Laws & Business, 2nd Floor, Monument House, 215 Marsh Road, Pinner, Middlesex HA5 5NE, UK. Tel: +44 (0)20 8868 9200
Fax: +44 (0)20 8868 5215, email: sales@privacylaws.com
web: www.privacylaws.com 5/02

**www.privacylaws.com**

## *Guarantee*

If you are dissatisfied with the newsletter in any way, the unexpired portion of your subscription will be repaid.