UNITED KINGDOM NEWSLETTER

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

IC's new power to impose fines

The Information Commissioner has been given the power to fine organisations for serious breaches of data protection principles. **Laura Linkomies** reports.

Organisations now face substantial fines for intentionally or recklessly committing serious breaches of the principles of the Data Protection Act. The Criminal Justice and Immigration Act, which received Royal Assent on 8 May, introduces in Section 144 a civil penalty rather than a criminal penalty that was adopted in an amendment by the House of Lords last month.

The Commons amendment says that a "data controller must not intentionally or recklessly disclose information contained in personal data to another person or repeatedly and negligently allow information to be contained in personal data to be disclosed".

Fines (to be paid into the Consolidated Fund) are applicable when organisations knew that there was a risk that the contravention would occur and that such a contravention would be of a kind likely to cause substantial distress or damage but failed to take reasonable steps to prevent the contravention. Fines are not applicable if the disclosure was necessary for the purpose of preventing or detecting crime, was required by law or was in the public interest.

More detail, including a maximum penalty, will be set out in ICO Guidance and regulations that will be published later by the Secretary of State. Organisations will be able to appeal to a Tribunal.

Although not what it asked for (the ICO had previously asked for a new criminal offence of knowingly or recklessly failing to comply with the data protection principles), the ICO welcomes the new Section 144 penalty.

David Smith, Deputy Information Commissioner, said: "This change in the law sends a very clear signal that data protection must be a priority and that it is completely unacceptable to be cavalier with people's personal information. The prospect of substantial fines for deliberate or reckless breaches of the Data Protection Principles will act as a strong deterrent and help ensure that organisations take their data protection obligations more seriously.

> "This sends a very clear message that data protection must be a priority."

"This new power will enable some of the worst breaches of the Data Protection Act to be punished. By demonstrating that the law is being taken seriously, tougher sanctions will help to reassure individuals that data protection is important and give them confidence that organisations have no choice but to handle personal information properly.

"The fact that strengthening the DPA has cross-party support demonstrates the growing consensus on the importance of effective data protection."

• *To see the House of Commons' amendments, visit web page www.publications.parliament.uk/pa/ld200708/ldbills/054/2008054.pdf.*

Issue 37 **JUNE 2008**

UNITED KINGDOM
newsletter
ISSUE NO 37 June 2008

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 Hendi +44 (0)20 7336 7300

ISSN 1472 9563

comment

Watch out for those insiders

Most data breaches happen when employees do not take proper care in handling or transferring personal data. In other words, no matter how good your security systems are, there is always that human factor. So everyone should be prepared to deal with data breaches.

The Information Commissioner encourages organisations to notify any significant breaches to his office, and has identified the information they need to receive to be able to give advice. While notification is not mandatory, in light of the number of data breaches that have occurred in the past year, it may well be in the future (p.9). The problem lies in what would be included in a breach notification law. Australia is considering, in its review of privacy laws, recommending civil penalties for failure to notify the Privacy Commissioner. However, it is proposed that notification would only be needed when a breach involves a real risk of serious harm to the individual. In the US, many states have introduced civil penalties for not notifying the individuals affected.

Proper records management is a key to good data protection compliance and should receive as much attention as improving security measures. In this issue, we look at how audits and records surveys can help you to comply with the Act (p.11).

A new database has been set up to warn employers of dishonest workers. An employee need not have a criminal record to be added to the database. Theft, forgery, causing damage to the company or falsifying documents could all act as triggers. From the data protection viewpoint, it is unfair to blacklist individuals when there has not been enough evidence to prosecute. There are also concerns over issues such as fair processing, and sensitive data. Read more on p.3.

We also look at the new penalties, fines and prison sentences for not respecting consumer opt-outs. Read more about enforcement synergies between the Information Commissioner and Trading Standards Officers on p.7.

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.

New employee database: solution to a genuine employment problem or a step too far?

Recording dismissals in a national database causes data protection concerns.
By **Nick Graham**.

A new database will go live this month that will hold the details of any employee who has left a job after having allegations of theft, fraud or similar offences made against them. It is called Action Against Business Crime, and is being established by a partnership between major retailers under the umbrella of the British Retail Consortium and the Home Office. Although the aim of the database is to warn future employers about suspect employees, many have raised substantial issues about it, in particular concerning data protection compliance.

The National Staff Dismissal Register

The purpose of the register is to reduce business costs and losses caused by dishonest employees and make the recruitment process more efficient by allowing employers to assess whether prospective employees have a history that they have not disclosed to their potential new employer.

The register will hold information on any employee who has been dismissed or otherwise left their role while under suspicion of:

- theft;
- fraud or forgery;
- causing loss to a company, its suppliers or customers; or
- causing damage to a company's property.

Employers will be able to search for data, including the employee's name, address, date of birth, National Insurance number and previous employer, and will be able to access the register online.

General concerns

The new register raises general concerns. Does the register reverse or dilute the principle that individuals are innocent until proven guilty? Does the register also open the door to the possible illegitimate manipulation of suspicions to force an employee to leave his or her job rather than the employer going through the standard dismissal process? Also it is not clear how long the register will retain the data in question, so allegations without any solid proof could turn out to be more damaging to an employee than an actual criminal conviction.

In addition, the Criminal Records Bureau (CRB) already exists to allow employers to check whether potential employees have criminal records, thereby relying on high standards of criminal law being met before an employee's record is tarnished. It is not clear how the register sits with the CRB.

Data protection

We understand that the Information Commissioner has been regularly consulted during the development of the register. However, there does seem to be a number of key data protection risks and issues that are relevant:

1. data protection law will require individual employees to be informed about the database and the purposes for which it may be used. This may be possible to do going forward but is much more difficult in relation to legacy employee data;
2. there is an open question as to whether any of the information would be "sensitive personal data", which would trigger a requirement to collect explicit consents from each employee;
3. the collection and use of the data will probably need to be within the former employers'/subscribers' "legitimate interests" (unless individual consents are collected) and must not involve any collection or use of data that is unwarranted by reason of prejudice to the rights and freedoms or legitimate interests of the relevant employees;
4. the database will also need to comply with general data protection principles. This means that data must be adequate, relevant and not excessive, kept up to date, and not kept longer than necessary.

Defamation risk

If an employer were to list an employee on the register without being able to justify the relevant suspicions, they may leave themselves open to risk of a

ICO STATEMENT

"The ICO has been consulted by Hicom Business Solutions and we have worked to ensure that data protection considerations are given adequate attention during the development of the National Staff Dismissal Register (NSDR). It is essential that any organisation which subscribes to the NSDR complies with the Data Protection Act. Organisations must inform employees when the NSDR is being used, both before checking an individual's status on the database and before entering an individual's details on the register. The Data Protection Act gives individuals the right to access information about themselves that is held on the database and to correct any inaccurate information. We are aware that the system provides for these rights to be exercised. If an individual is unhappy with the way in which their information has been processed, they should raise their concerns with the organisation which is processing the data in the first instance. If they continue to dispute their inclusion on the database, individuals have the right to complain to the Information Commissioner's Office."

defamation claim. Interestingly, many employers no longer give detailed references in relation to employees. However, use of the register seems to involve a step back to the days when prospective employers would be provided with more detailed information about prospective employees. Again, one of the reasons for the change was to avoid the defamation risk, which therefore may rear its head again.

What does it all mean?

The new register is one of the many new databases being created to allow commercial parties (and, in other cases, government departments) to share data and use it more effectively. However, it does seem to represent a cultural shift from the traditional position in relation to the giving of employment references.

Also, a number of data protection issues seem to arise, together with associated employment law risks. Participants and subscribers should ensure that their particular use of the register is compliant.

AUTHOR

Nick Graham is a partner at law firm Denton, Wilde, Sapte.
E-mail:
nick.graham@dentonwildesapte.com.

ICO criticises phone call and e-mail database

The Information Commissioner has criticised Home Office plans to introduce a database of electronic information that will hold details of every phone call and e-mail sent in the UK. Although the plans are provisional, they are meant to be included in the Communications Bill later this year. A Home Office spokesman said the data was a "crucial tool" for protecting national security and preventing crime and that changes need to be made to the Regulation of Investigatory Powers Act 2000 "to ensure that public authorities can continue to obtain and have access to communications data essential for counter-terrorism and investigation of crime purposes".

However, the ICO feels that these plans jeopardise individuals' privacy. Assistant Information Commissioner Jonathan Bamford said: "If the intention is to bring all mobile and internet records together under one system, this would give us serious concerns and may well be a step too far.

"We are not aware of any justification for the state to hold every UK citizen's phone and internet records. We have real doubts that such a measure can be justified or is proportionate or desirable. Such a measure would require wider public discussion. Proper safeguards would be needed to ensure that the data is only used for the proper purpose of detecting crime.

"We have warned before that we are sleepwalking into a surveillance society. Holding large collections of data is always risky; the more data that is collected and stored, the bigger the problem when the data is lost, traded or stolen. Defeating crime and terrorism is of the utmost importance, but we are not aware of any pressing need to justify the government itself holding this sort of data. If there is a problem with the current arrangements, we stand ready to advise on how they can be improved, rather than creating an additional system to house all records."

Code on data matching practice

The Audit Commission acquired a new statutory power in the Serious Crime Act 2007 to conduct data matching exercises for the prevention and detection of fraud, and thus the Commission is now preparing a code of practice.

The purpose of this code is to help ensure that the Commission and its staff, auditors and all persons and bodies involved in data matching exercises comply with the law, especially the provisions of the Data Protection Act 1998, and to promote good practice in data matching. It includes guidance on the notification process for letting individuals know why their data is matched and by whom, the standards that apply and where to find further information.

Consultation on the draft code, which has been drafted with the help of the Information Commissioner's Office (ICO), ended on 30 May.

• *The Audit Commission Draft Code is available at web page www.audit-commission.gov.uk/nfi/consultationcode. The ICO's Framework code of practice for sharing personal information is at www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/pinfo-framework.pdf.*

Human factor is biggest threat to data security

A survey by InfoSecurity Europe that asked individuals to part with personal data in exchange for sweets and the possibility to win a holiday reveals that companies should be alerted to the threat of data leaks by staff.

The survey, carried out at Liverpool Street Station in London in April, asked for personal information from 575 people. The interviewees gave their names, telephone numbers and passwords. One in five was happy to part with their passwords. In a similar survey in 2007, the result was a staggering 64%. None of the information collected by the research was used or saved.

"Other key principles of the Act include ensuring personal information is accurate and up to date and that it is used for purposes which people have been told about. By following these simple principles, businesses can ensure they provide an effective customer service. What business wants to irritate people and incur costs by sending marketing information to people who clearly don't want to receive it?

"The Act gives us important rights and protection in an age where more and more of our personal information is being collected and traded. We should recognise the benefits it brings, not belittle it as a burden."

However, 28.2% of the 300 UK companies that were interviewed for a recent Eurobarometer survey say that they rather agree that "the requirements of the data protection law are too strict in some respects. One third thought that DP regulations were not needed except for certain sectors or activity. The interviews were conducted in January 2008.

Ten councils to share access to confidential data

A group of local authorities are starting to use Microsoft's digital identification to share personal data between themselves, reports Znet.com (18 April 2008). The councils will use their online identities to share internal documents relating to the group. A dedicated portal will allow for the secure sharing of documents as well as taking part in discussions relating to the group.

The local authorities taking part in the project are Newham, Bromley, Derby, Isle of Man, Kent, Lewisham, Rotherham, Sunderland, Wakefield and Warwick. They form the Shared Learning Group, which looks for innovative IT solutions to deliver customer-centric, efficient and effective public services. Identity management that will simplify citizens' access to services is on the government's "transformational government" agenda.

Geoff Connell, chief information officer at Newham, said: "Recent security breaches have highlighted the need to enhance IT security in governmental organisations. Using [Microsoft's virtual] information cards makes it easier for the group to share information in a secure manner."

Data breaches force HMRC to punish staff

HM Revenue and Customs (HMRC) had to discipline or dismiss 192 of its workforce of 90,000 people in 2007 in incidents involving inappropriate access to personal or sensitive data.

Replying to a Parliamentary Question on 30 April, the Treasury Financial Secretary Jane Kennedy revealed that 238 staff were disciplined at HMRC in 2005 and 180 in 2006. Kennedy also said that since 2005, HMRC has had to report 11 data-security breaches to the Information Commissioner.

ICO says DPA is not burdensome

The 2008 British Chamber of Commerce's Burdens Barometer report called for a number of "burdens" to be reviewed, including the Data Protection Act. The ICO has reacted to this report by saying that, according to its research, 90% of businesses believe that DPA is needed and adds value to their business rather than extra burden.

The ICO says: "In recent months the importance of the Data Protection Act has never been so obvious. Recent security breaches have reinforced the need for all organisations to ensure personal information is secure. This is a key principle of the Act. If businesses fail to properly safeguard information, they risk losing the trust and confidence of their customers.

UK organisations say DP law rather strict

Two thirds of UK organisations think that the requirements of the DP law are too strict in some respects. However, the European Commission's Eurobarometer survey on data controller's perceptions about data protection in Europe also reveals that 40 % of UK companies think that that the existing legislation on data protection is rather well suited to cope with the increasing amount of personal information being exchanged, for example transferred over the Internet. Less than one in three thought that the requirements of data protection law are not necessary except for certain sectors of activity. 29% rather agree that there is sufficient harmonisation of Member States' data protection laws to consider that personal data can be moved freely within the European Union. However, 15.5% of UK respondents totally disagree with this statement. Nearly half of the respondents thought that data protection law was applied more rigorously in the UK than in other EU Member States.

The results based on responses from all Member States indicate that the majority would favour greater harmonisation of the security measures while the least favoured action would be the development of sector specific measures. In addition,

- Eight out of 10 respondents were in favour of making national laws with respect to information provided to data subjects more uniform across the EU.
- Seventy-eight percent agreed with the aim of having a better balance

between the right to have your data protected, and freedom of expression and information.

A lower proportion of 76% would welcome further clarification on the practical application of some of the key definitions and concepts of the European Directive and national DP laws.

The survey, compiled in January 2008 and published in February 2008, presents average results from the 27 EU Member States, results for each separate country and results by company category. The UK results are based on interviews with 300 UK companies.

ICO's recommendation for Department of Health

The ICO has issued, having completed an audit of complaints concerning the Department of Health (DoH), a Practice Recommendation that addresses the organisation's FOI compliance.

The Department of Health was served a Decision Notice on 21 January 2008, which included several concerns about the organisation's failure to disclose contract information.

The current audit, which looked at the management of 40 FOI requests, suggests that the Department has failed to offer appropriate advice and assistance to applicants and to transfer requests appropriately. It had also delayed the internal review process beyond a reasonable timescale. At the time of issuing the Practice Recommendation on 31 March, the delay resulting from these extensions amounted to more than 90 working days.

The ICO says: "The Department repeatedly applies blanket exemptions to requested information with the effect of withholding entire documents from release. This suggests that rather than considering requests on their own merits, exemptions have been applied on a general principle. The Commissioner is concerned that the application of exemptions in this way may have the effect of suppressing non-exempt information from release."

The ICO lists many recommendations on how the organisation should improve its FOI compliance. For example, the DoH should ensure that it has a central core of staff with particular expertise in Freedom of Information who can provide expert advice to other members of staff as needed. The Commissioner also points out that the department should review their complaints handling procedure, and ensure that consultation with third parties is carried out at the earliest opportunity.

A Practice Recommendation is not enforceable, but a failure to comply with a Practice Recommendation may lead to a failure to comply with the Act, which in turn may result in the issuing of an Enforcement Notice.

• *See www.ico.gov.uk/upload/documents/library/freedom_of_information/notices/1221758_4_doh%20v4.pdf.*

ID card review by OGC case back to Tribunal

The High Court has overturned the Information Tribunal's decision on whether ID Gateway Reviews by the Office of Government Commerce (OGC) should be published (*PL&B UK*, July 2007, pp.14-15). The case has been sent back to the Information Tribunal, which will re-assess the case. The High Court ruling says that the Tribunal was mistaken in relying on the findings of a Parliamentary Select Committee on Work and Pensions, as this puts the Tribunal and the judiciary at risk of breaching Parliamentary privilege – courts are forbidden to pass judgements on Parliamentary decisions.

• *The ruling, made on 11 April 2008, can be seen at web page www.bailii.org/ew/cases/EWHC/Admin/2008/737.html.*

Model publication scheme now available

The ICO has published a model publication scheme to aid public sector organisations comply with the FOI Act's requirement to adopt and maintain a publication scheme. The model scheme may be adopted by any public authority from 1 January 2009 without any modification. No further approval is necessary, and it will be valid until further notice. It lists classes of information for publication, organisational information, financial information, strategy, performance information, reviews and assessments, decision making, policies and procedures, lists and registers and the services offered. In addition, organisations should provide details of the method under which they publish information, any charges they make, and how to apply for more information in writing. The ICO has also produced a series of definition documents for each sector which identify the type of information they would expect to see included in each class.

The move follows an ICO review in 2005 which concluded there was a need to develop and improve the proactive dissemination of public sector information, and adopt a consistent approach. Approval of all existing schemes has been extended until 31 December 2008. The Information Commissioner will be writing to public sector Chief Executives to urge them adopt the new model publication scheme.

• *To see the model publication scheme, go to web page www.ico.gov.uk/Home/what_we_cover/freedom_of_information/publication_schemes/publication_schemes_eng.aspx.*

New consumer protection rules: Big fines and jail for breaches

New regulations in force from 28 May mean that firms need to pay more attention to respecting consumer opt-outs, and that there is likely to be closer cooperation on enforcement between the ICO and Trading Standards Officers. **Asher Dresner** reports.

The Consumer Protection from Unfair Trading (CPUT) Regulations 2008 that ban 31 practices in direct marketing pose a threat to companies of a prison sentence or a maximum fine of £5,000 if they fail to adhere to them.

One of the banned practices is "making persistent and unwanted solicitations by telephone, fax, e-mail or other remote media except in circumstances and to the extent justified to enforce a contractual obligation".

Janine Paterson, Legal and Public Affairs Advisor at the Direct Marketing Association (DMA), said: "Companies ignoring the telephone preference service (TPS) and persistently calling numbers registered on the scheme have got away lightly. Now, however, they could face prison if they continually call numbers against the consumer's wishes. The DMA welcomes this new legislation and is advising members on this and other elements of CPUT Regulations and the Business Protection from Misleading Marketing Regulations."

Similar legal protection may also be afforded to the subscribers to the mail preference service, if "other remote media" will be defined to include direct mail.

New era

The consumer protection regulations also herald a new era of stronger cooperation between the ICO and local trading standards officers (TSOs) backed by the Office of Fair Trading.

Few data protection managers know that Information Commissioner Richard Thomas is Vice-President of the Trading Standards Institute (TSI). More than of symbolic value, there are powerful synergies between the TSI and the ICO based on mutual interests in defending consumers.

The result is that while data protection managers and their legal advisors are accustomed to interacting with the Information Commissioner, they now need to face up to a new and additional regulator, or rather 203 of them across the UK: local TSOs. They are limbering up to play a more active role in the enforcement of data protection law, as TSI's Deputy Chief Executive Paul Ramsden explains to Stewart Dresner for *PL&B UK*.

The new consumer protection regulations update the Trade Descriptions Act 1968 and implement the EU Unfair Commercial Practices Directive (2005/29/EC). The UK regulations list 31 banned practices, some of which are similar to, or help promote, data protection principles, for example:

- Regulation 5, misleading actions, false and untruthful information likely to deceive a consumer (similar to the data protection principle of fair and lawful processing)
- Regulation 6, misleading omissions, and information that is unclear or unintelligible (similar to the data protection principle of fair and lawful processing)
- Falsely claiming a trust or seal mark when an organisation does not hold it (will be useful once the European Privacy Seal takes off – see *PL&B UK*, February 2008 pp.12-15).

The new Consumer Protection from Unfair Trading Regulations 2008 potentially broaden the extent of what is unlawful in the unlawful processing element of the first data protection principle: "Personal data shall be processed fairly and lawfully."

ICO's audit role for TSOs?

The Information Commissioner's Office (ICO) has only four or five auditors to

THE ROLE OF TRADING STANDARDS

The 203 Trading Standards Services around the country enforce a range of consumer protection laws and prosecute where necessary. Trading Standards Officers (TSOs) enforce laws relating to fair trading, consumer safety, weights and measures, consumer credit, underage sales, food safety and animal health and welfare. Now consumer protection aspects of data protection law are on the agenda.

TSOs defend consumers against unfair trade practices

TSOs exist to defend the rights of consumers against unfair or misleading trade practices. In recent years, there has been a focus on combating scams and money laundering, involving targeted schemes such as "scambusters", and dedicated units to combat money laundering, initially piloted in Birmingham and Glasgow and now operational across the country.

In recent years, the Trading Standards Institute has concentrated on piecing together the disparate intelligence it receives from its 203 regional Trading Standards offices, in order to better target its resources.

Paul Ramsden, Deputy Chief Executive of the Trading Standards Institute, the trading standards support and training body, cites intellectual property crime (such as patent abuse or illegal sales of copyrighted original works) as an example of an area in which intelligence benefits TSOs. He explains that the government has recently invested more into enforcement in this area, in the wake of the Gowers Review of Intellectual Property. Traditionally, a tip-off about the sale of illegally copied CDs, for example, may have enabled TSOs and police to arrest one seller, but that would likely have been of limited use to TSOs in terms of intelligence, as the seller would be unlikely to know much useful information about the identity of his supplier. But by sharing information between regional Trading Standards services about, for example, other sightings of suppliers which match the seller's description of his supplier, sellers higher up the chain may be identified and arrested.

enforce data protection legislation. However, Ramsden states that TSOs could play a role in helping the ICO with enforcement in future. The TSOs' role has already started to encompass areas that might better be described as auditing rather than inspection, and they already help other regulatory bodies. Two examples are areas that involve the processing of personal data.

1. **Credit licensing rules**. Any business which offers credit or lends money must be licensed by the Office of Fair Trading (OFT), which in turn has a duty continually to monitor the fitness of those holding or applying for licences. In recent years, TSO's roles in credit licensing has grown. Traditionally, TSOs were just required to comment on any parties applying for or renewing their credit licences. Now, the OFT contracts with the TSO in the relevant region, which then actively audits applicants for a credit licence and then reports back to the OFT. This provides a useful precedent and model for the potential use of TSOs in data protection enforcement work for the ICO in two ways: they are auditing, as oppose to carrying out traditional inspections, and they are doing so on behalf of another regulatory body, the OFT.
2. **The OFT's money-laundering regulations** is another area in which TSOs have taken on an audit function. Estate agents are required to confirm the identity of their customers, keep an eye out for transactions which indicate that the customer may be using property to launder money, and keep records pertaining to the customer's identity and relevant business transactions. This responsibility requires regional TSOs to shift their thinking from traditional inspections of a business property to support law enforcement to the auditing of business procedures to support compliance, in a similar way to data protection audits. Like the data protection regulatory regime, estate agents must sign up to a money-laundering register, part of a programme to prevent innocent estate agents unwittingly laundering money.

Benefits for firms' DPA awareness

Unlike the ICO's data protection auditors who require the consent of the data controllers, TSOs can carry out compulsory inspections and audits. When they help to enforce data protection law, the Data Protection Act too would be brought within that framework of compulsory audits. Clearly the enforcement regime would be strengthened through the Regulatory Enforcement and Sanctions (RES) Bill (see *PL&B UK*, April 2008, pp.15-16), including the DPA, once the RES law has been adopted by Parliament, expected by 1 October 2008.

The result would be that TSOs would have far more generalist auditors available, with stronger powers than the small number of specialist ICO auditors.

Ramsden agrees that this increase in audit resources would provide a powerful incentive for firms to ensure that they understand their obligations under the DPA. Part of Trading Standards' remit is to inform and educate both firms about their obligations and consumers about their rights. TSOs could be powerful partners in helping the ICO to educate firms about their obligations under the DPA. Firms often do not have specific questions about certain areas of law; they just want to know what it is that they need to know. That could include DPA requirements. "Often businesses need tailored inspections and an assessment of their particular compliance needs," he explains. "Inspections are all well and good, but really assessments and advice are necessary. A data protection section may be appropriate for the TSI website, as firms go there for information about the range of things they need to comply with."

Consumer Direct

The TSI also has the means to advise consumers who believe that their personal data is being misused. Ramsden describes the provision of advice to prevent dishonest and illegal practices as "the *raison d'être*" of TSOs, and the Consumer Direct telephone advice service as "the customer-facing side of Trading Standards... recognising other issues and referring them on." All Consumer Direct advisers are members of the TSI, and there are 11 regional centres around the country that deal with myriad consumer issues. This provides an opportunity to raise awareness about data protection issues via a well publicised national advice service, in 11 regional centres, funded by the OFT.

DP audit accreditation

To take on data protection auditing responsibilities, TSOs would need accreditation and extra training. Here again, though, Paul Ramsden explains that audit training already forms part of the standard training that TSOs must undergo. He explains that there is an option within the formal training to take a lead auditor qualification, but the standard training regime does include an important quality assurance element. This is an important part of the standard training because a standard defence used by companies that are either accused of or charged with trading standards offences is that the offence for which they have been caught is a one-off, and they do, in fact, have controls and procedures in place to prevent illegal practices. This is known as the "due diligence" defence. This means that as well as assessing companies for their compliance with all relevant trading standards legislation, trading standards officers also need to be able to assess in advance whether this

TRADING STANDARDS OFFICERS' ACCESS TO DATA

As part of an investigatory body, TSOs are now subject to the constraints on what information they can obtain, as set out in the Regulation of Investigatory Powers Act 2000 (RIPA).

This has led to a reduction in the number of requests made by TSOs for information. Mr Ramsden explains that often information is obtainable by other means, or by piecing other evidence together. He also explains that because the procedure for the release of information using investigatory powers is broadly the same irrespective of the nature of the information, TSOs often find that channel unduly burdensome for the nature of the information they are seeking. This is not helped, in his opinion, by the divergent views of the English, Scottish and Welsh Surveillance Commissions on applications for information.

The regime has been successful inasmuch as he says he is not aware of any complaints about invasions of privacy resulting from TS investigations.

likely defence rings true, which requires an audit procedure. They must assess the company's system, whether it is being taken up across the whole company, whether it works in all areas, whether it is effective, and so on.

Clearly, however, training on the DPA requirements would be necessary for TSOs, as these are not areas which are currently common in their daily work.

ICO cooperation

Taking on data protection auditing skills and concerns would be extra work for Trading Standards. What might they gain? Mr Ramsden explains that often organisations that are suspected of serious illegal activity can be taken out of business if they are found guilty of less serious legislative breaches that TSOs enforce. "One of the things we keep trying to reinforce with other partners is the fact that we should get together and identify a criminal," he says, "and if there is real suspicion around heinous crimes like smuggling or drugs, arrest them for counterfeiting CDs. Then you can assess their criminality ... and if they can't prove they've got [their assets] from legitimate means, seize cars and houses."

Partnerships with other regulators are useful in this respect, he says. To that extent, the TSI looks out for organisations to partner with, and helping to enforce data protection law may bring benefits to Trading Standards, in terms of tackling suspected rogues. "There are many existing partnerships," he explains, "and it's a case of not being precious about who it is that takes them out. Ultimately, the focus is around consumer protection and ensuring that companies compete in a good honest competitive environment. [Where] you can identify wrongdoing which doesn't necessarily fall squarely within the framework of trading standards, we look at the partnerships which are best to deal with it."

TSOs' strong powers

TSOs have relatively strong powers that would be available in the service of the data protection laws if the ICO and Trading Standards were to cooperate. Their powers are tiered. Ramsden explains that they have "quite strong" powers to investigate reports of rogue traders, and then a separate set of powers to take action if they have reasonable cause to suspect illegal activity.

For example, unlike the police, TSOs have the power to enter any premises that they believe to be a front for counterfeiting activity – without a warrant. This includes residential properties, provided they have evidence that a business is being run from inside. In practice, a warrant for entry is normally obtained, as it is a practice that is better accepted and because it puts the operation on a more secure footing if the police are involved. As police have powers of arrest and TSOs do not, inspections with intentions to arrest or capture evidence are normally accompanied by a police officer. This means that where criminality has been established, an arrest can be made without giving the suspect the chance to become aware of the investigation and remove evidence of illegal activity.

The new legislation gives TSOs additional powers but also standardises regulatory enforcement across local authorities by empowering the Local Better Regulation Office to appoint one authority as the "primary authority", mandating it to deal with companies that are in breach. Ramsden explains that this face-to-face contact between representatives of a company and local authorities nationwide will establish greater mutual understanding and trust. "Where the legislation isn't black and white," he says, "there's some potential to explain how they should do certain things." This kind of contact could improve data protection awareness and auditing too.

Tackling new issues

Because of both their audit training and their increasing awareness of the DPA, TSOs are increasingly well-equipped to help the ICO with enforcement of the Act in the future. Ramsden is clear that TSOs have an appetite for tackling new issues. While the OFT takes responsibility for the consumer law review on electronic communications, "whether children give their consent to the use of their information when communicating online is something we could certainly look at". As for the risk of privacy intrusion represented by marketing via mobile phones and by Bluetooth, "the TSI recently held a seminar on anticipating tomorrow's problems. It's a potential area for an information exercise. Consumers are going to start complaining, and we can do something before they complain."

AUTHOR

Asher Dresner is a PL&B correspondent

Rise in data breaches paves way for mandatory notification

With up to 60% of UK businesses experiencing data breaches, the ICO has published guidance on how to deal with these incidents. **Laura Linkomies** looks at recent developments.

A recent Ponemon Institute survey of nearly 650 UK-based IT and business managers suggests that two thirds of businesses in this field have lost personal data over the last 12 months. This supports earlier *PL&B* survey findings, based on responses from a cross-section of companies, that one in three has suffered a data breach in 2007 or early 2008 (*PL&B UK*, April 2008, p.1).

The Information Commissioner's Office (ICO) has confirmed the trend by saying that since the security breach at HM Revenue and Customs in November 2007, almost 100 data breaches have been notified by public, private and third-sector organisations. In terms of breaches notified to the ICO by private-sector organisations, 50% were reported by financial institu-

tions. Of those reported by public bodies, almost a third occurred in central government and associated agencies and a fifth in NHS organisations.

Commenting on these figures, Information Commissioner Richard Thomas said: "It is particularly disappointing that the HMRC breaches have not prevented other unacceptable security breaches from occurring. The government, banks and other organisations need to regain the public's trust by being far more careful with people's personal information. Once again, I urge business and public sector leaders to make data protection a priority in their organisations. The level of understanding about data protection and the need to safeguard people's personal information have no doubt increased, and I am encouraged that more chief executives and permanent secretaries appear to be taking data protection more seriously, but the evidence shows that more must be done to eradicate inexcusable security breaches."

Why notify the ICO?

The ICO encourages organisations to come clean and tell them about serious data breaches that can potentially harm individuals, for example by exposing them to identity theft. However, if the information is publicly available anyway, or the information that is lost is encrypted, there is no need to inform the ICO. The ICO also says that the volume of lost details affects the need to notify, as well as the sensitivity of that data. If "only" some 500 records from a marketing list are lost, the ICO does not need to be informed. On the other hand, if the breach involved details of more than 1,000 individuals, voluntary notification is recommended. Losses of particularly sensitive data need to be reported regardless of the numbers affected.

When an organisation decides to report a security breach, the notification should include the following information;

- The type of information and number of records
- The circumstances of the loss/release/corruption
- Action taken to minimise/mitigate the effect on individuals involved, including whether they have been informed
- Details of how the breach is being investigated
- Whether any other regulatory body has been informed and its response
- Remedial action taken to prevent future occurrence
- Any other information you feel may assist the ICO in making an assessment.

So why would organisations voluntarily give out information that may cause them to be named and shamed? The ICO will give advice on how to best handle the situation and avoid similar breaches happening again. It will not publicise the breach but may strongly recommend that the organisation involved does so, especially if there is a strong public interest in doing that. However, the breach will become public knowledge if the ICO is forced to take regulatory action, typically if negotiations with the organisation have failed. Sometimes the ICO may simply make note of the breach if it is not particularly significant. It is worth remembering that the ICO can now impose fines (see p.1). And it is likely, after an investigation, to recommend changes to the organisation's data security, for example to introduce encryption.

The ICO thinks that there should also be heavy penalties for not notifying after a breach. Otherwise, the corporate risk of notifying might be seen as greater than the risk of not notifying. There is also the other side of the coin. The ICO warns companies of the dangers of "over-notifying". There is no need to inform the whole customer base if the breach affects just some people. Also, notifying every little incident may make people too complacent.

Christopher Kuner, Partner at the law firm Hunton & Williams, agrees: "One of the main problems of the US data breach legislation is that in many cases it sets the threshold for breaches that must be notified too low. But it is difficult to come up with a clear definition of where the threshold should be set.

"Clearly the law in the US has made organisations more aware of IT security obligations. But I suspect that many of the incidents that have come to light have always been happening, it is just that the law has brought them to light."

Kuner also notes that penalties should be stringent enough so that they produce real compliance. However, as experience has shown, publicity about a breach can be even more damaging than legal penalties.

Cost of notifying

Notifying does not necessarily cost much, but the implications of data breach do. According to a recent study by the Ponemon Institute, the cost related to notification itself was the least significant, averaging only £1 per record. However, when managing a data breach, the total cost per compromised or lost record was £47. While that may set alarm bells ringing, it is worth noting that the average total cost per company was more than £1.4 million per breach (however, this ranged from £84,000 to almost £3.8 million). Lost business makes up for the biggest part of costs. According to the study, this averaged more than £496,000 per business, or £17 per record compromised. Other costs include, for example, legal costs, improvements in technology after the breach, and measures to regain consumer trust.

The study, which is based on interviews of 21 UK companies that had experienced data breaches, also revealed that the loss or theft of laptops and mobile devices were the most frequent cause of a data breaches. A staggering 38 per cent of breaches occurred when data was held by third parties, and most data breaches occurred in the financial sector.

Regulation on the cards?

So what are the chances that future data breaches will by law have to be reported? The ICO seems supportive of the idea of a data breach law. In its response to a *PL&B* survey, the authority said that above all, it wants clarity of purpose and scope: what is the law intended to achieve and how would it operate? The ICO stresses that such a law should apply to both private and public sectors, and there should be compensation to individuals where appropriate.

But there are no new developments in terms of regulation. The House of Lords Science and Technology Committee's report on security on the Internet in August 2007 recommended some form of breach notification to

protect Internet users, but the government has not yet taken any steps towards regulation in this field, partly due to uncertainty over whether it would make a difference. Even the ICO has warned that if a law is adopted, it must be well drafted, workable and understandable to business.

European initiatives

On the European level, there is support for security breach notification. European Data Protection Supervisor (EDPS) Peter Hustinx said in his opinion of 10 April 2008 on amending the Privacy and Electronic Communications Directive (2002/58/EC) that the new breach notification duty should not only apply to the telecommunication field, but also to other actors, especially to providers of information society services which process sensitive personal data (such as online banks and insurers, and online providers of health services).

Hustinx says that security breach notification enhances accountability and has a positive impact on security investment. He states that "the simple fact of having to publicly notify security breaches causes organisations to implement stronger security standards that protect personal information and prevent breaches. Furthermore, the notification of security breaches will help to identify and carry out reliable statistical analysis regarding the most effective security solutions and mechanisms. For a long time there has been a shortage of hard data about information security failures and the most appropriate technologies to protect information. This problem is likely to be solved with the security breach notification obligations."

The European Commission has recently invited tenders for a study on different approaches to new privacy challenges. The Commission is looking for guidance on whether the legal framework of the Directive provides appropriate protection or whether amendments should be considered. It may well be that this will, among other things, test the climate for breach notification. Also, the UK Commissioner has launched a study into how the EU DP Directive could be modernised.

Amending the Directive would, however, be a slow process, and not without difficulties. "Article 17 of the Data Protection Directive mandates security measures," says Kuner, "but doesn't say anything about notifying them. Articles 10 and 11 and the Directive mandate that certain information about data processing be given to individuals. It is probably these articles that are the hook into a breach notification requirement, rather than Article 17. While security breach isn't mentioned in Articles 10 and 11, there is no reason why a Member State couldn't go beyond the Directive and introduce this at a national level. Of course, an EU-wide rule would be preferable, to avoid fragmentation of the law around the EU," says Kuner.

INFORMATION

See ICO Guidance on security breach management at www.ico.gov.uk/upload/documents/library/data_protection/practical_application/guidance_on_data_security_breach_management.pdf.
Serious breaches should be notified to the Information Commissioner's Office at mail@ico.gov.uk
EDPS statement www.computing.co.uk/computing/news/2214243/ec-should-further-privacy.
The Ponemon 2007 Annual Study: UK Cost of a Data Breach, Understanding Financial Impact, Customer Turnover, and Preventitive Solutions, was published in February 2008. See www.ponemon.org.

Where records management meets data protection

With the ICO getting new powers to impose fines on organisations that deliberately or recklessly commit serious breaches of the Data Protection Act, proper records management has never been more important. **Alison North** explains how audits, information gathering and records surveys can help.

Good records management ensures the systematic management of all records and the information they contain throughout their lifecycle. Of the eight data protection principles in the Data Protection Act, at least 3 of them cross over into records management territory.

Records Retention relates to the data protection principle that personal data is "not kept longer than is necessary". Records Management is responsible for developing and implementing records retention schedules defining periods of time for keeping records in line with the legislation of the jurisdiction in which your organisation operates as well as your sector's regulations and codes of practice:

Records Security is quite often more focussed on paper documents and records, but more and more with electronic records, the records management function advises on methods for controlling all records and ensures that the archived records are "secure" and not easily accessed by an unauthorised person:

"For transfer of records to (other offices in) other countries", the records management function may be responsible for retrieving and transferring archived and semi-active records for their organisations and delivering them to other offices in a secure and protected environment.

Audits, information gathering and records surveys

Records Managers have been carrying

out Information Audits for many reasons for many years. We spin them according to the latest information management "hot spot". My distaste of this spin is appeased somewhat by the value of completing an information audit regardless of its underlying reason. That is provided it is an audit and not an information gathering exercise relating to statistics about your records. The two, along with a third, "the Records Survey", have all been referred to as "Audit" and are confused frequently by in-house records managers, external consultants and service suppliers alike. All three have their value in terms of Records Management (RM) but whilst a (real) audit and a records survey can assist with compliance in relation to the Data Protection Act, an information gathering exercise is more about numbers; how many, where and in what type of cabinet system your records are held, rather than an evaluation against your records management policy and its application within your work processes and procedures.

> It is no good developing an audit relating to records affected by data protection if your organisation has not developed a strategy to handle records in general.

What is an audit?

An audit by definition requires a set of rules by which the subject matter of the audit, in this case information, can be measured. At its most basic, an audit is performed to ascertain the validity and reliability of certain information and to provide an assessment of your organisation's internal controls relating to the specific subject. This means that to qualify the word Audit with the word Information may in fact seem meaningless unless we qualify the sort of Information we are seeking to audit. It is far better to call an audit relating to records management a "Records Audit", and one relating more specifically to Records affected by the Data Protection Act an "Audit for Records affected by Data Protection". Perhaps I am splitting hairs, but you get my pedantic drift I am sure. Making it more specific to the subject to be evaluated will make it easier to develop the checklist and set of rules against which the audit findings can be measured.

There is one very important aspect to consider before launching yourself into an audit. It is no good developing an audit relating to records affected by data protection (DP) if your organisation has not developed any sort of strategy / policy or processes to handle your organisation's records in general. A DP Records Audit can only be undertaken if you have a set of records management rules to measure the DP Records Management against.

Records survey

The first step in the absence of any records' controls is a Records Survey, the third, but possibly most important in terms of records management, in the list of confusion mentioned in the second paragraph. The Records Survey will gather information about your work processes and the records within them. It will ascertain just how your colleagues are handling their records and specifically, in relation to Data Protection, identify where the personal and sensitive data is contained within the many records held in your organisation.

During the survey it is important to gain a complete understanding of your organisation's "business", its objectives, new initiatives that may impact on DP and RM, its culture, its attitude to rules and regulations, its staff (your colleagues) and the level of risk it is comfortable with. Whilst these latter non-records points may seem unconnected to RM, they are not. It is impossible to develop a clear RM strategy without understanding your organisation and the way it works inside out.

Thereafter, a strategy that flows and links into the other strategies within your organisation is developed, taking all your findings and non-records' points, listed in the previous paragraph, into consideration. The strategy is then underpinned by the records management policy and guidelines that are drafted to support the organisation's objectives and "business" that is at its heart. The policy then has to be implemented with appropriate assistance consisting of training and guidelines, possibly toolkits to be developed. Not until all of this is in place and been operating across all of your organisation for more than six months can you really schedule and carry out a records audit.

That is not to say that you cannot improve on the way you handle personal and sensitive data right away. Having discovered where it is held and who is holding it, you can put in measures to remove data from areas where it should not be held and secure the data in the appropriate place whether that place is electronic / paper or both. Once your records management system is in operation all personal and sensitive data will be handled in a uniform manner by the correct staff, for the right reasons, over the correct period of time and in accordance with all the legal and regulatory constraints.

What stage are you at records audit or records survey?

The answer in my terms is obvious. If you do not have a records management strategy and policy and there are no processes for handling your records throughout their life cycle i.e. from creation through use to disposal, then you need to complete a records survey to assist you with data protection compliance. If you already have a records management strategy with a clear policy that has been implemented across your organisation, then complete an audit measuring the three DP principles relating to RM against your RM policy. The type of audit will depend on how your organisation has structured its data protection policy and the remit that you have given your Data Protection Officer. If RM and DP sit together, then the records and data protection audits can be combined. If, however, your DP is part of another function or sits alone, then the DP audit may need to extract those elements of the records audit that relate to the eight principles into the DP audit.

Whichever stage you are at, survey or audit, you are about to undertake a

Project. Do you have a time and a budget for the work? Do you have the expertise to develop and undertake this work completely in-house or do you need assistance from external consultants or other service providers?

In-house audit versus external consultant's audit

I am great proponent of "empowerment". I really like to see people learn and grow with new skills and knowledge so my answer to in-house audit v external consultant's audit is definitely both. Let me explain. An in-house auditor understands the ethos of their organisation: ultra modern or slightly old fashioned, driven from the top down or run by the middle managers, lean and mean or staff with little to do. They also have knowledge about how their organisation operates. By that I mean its method for following procedures/ enforcing regulations/adapting to change/spending money/ listening to, accepting and acting upon a consultant's advice, the latter being very important in this case. If your organisation is prone to paying for a consultation and then not acting upon it, hiring an external consultant to undertake an audit is a waste of money and time.

Using "empowerment" methods relies upon the consultant facilitating small meetings with groups of staff across the organisation, listening to them, understanding their issues, their fears and their ideas. Working with them to develop and implement their ideas, leading them to deliver the Records or DP project within a project management framework.

Will your (records) project succeed?

You may have wondered why I dwelt on the differences between records audit, information gathering and records survey. Your project will succeed if you know the difference and understand the purpose of each. Choosing the one most appropriate to your situation is very important if you wish it to succeed and assist with DP compliance too. CONFUSION is one of the main reasons why records management projects fail. Remove the confusion by clearly stating what the project aims to achieve, why you need to complete the project and how you are going to complete it. Your colleagues need to know this to support you and to provide the answers to your audit or survey.

There are other reasons why projects fail such as lack of management / staff commitment, no budget, poor project management skills, no implementation experience. These matter not if you don't clarify the terms of your project from the beginning.

And finally

This is a short article in which to discover a connection between records management and data protection. The two subjects are linked, as discussed at the beginning, in several ways, retention of records; security of records; transfer of records. Data Protection officers and Records Managers should work together to achieve compliance in the most effective way. Undertaking a records survey is a positive start and will identify areas of non-compliance that you can "fix" right away. An audit means you have a policy and processes in place that can be measured and will show clearly that your organisation is aware and follows the Data Protection Act principles in terms of Records Management.

AUTHOR

Alison North is Managing Director of the Genuine Group, an information management company focused on facilitating organisations to achieve compliance with the many legislative and regulatory requirements worldwide, through records management
E-mail: Alison.north@genuine-group.com

USEFUL LINKS

www.doc-law-regal.co.uk
www.jiscinfonet.ac.uk/infokits

It's monitoring, but not as we know it

Employee monitoring is a subject that causes most employers to stop and take note – everyone knows that you can't just start monitoring your employees without giving it some thought. **Valerie Taylor** reports.

There are obvious examples of employee monitoring – the CCTV camera above reception; the notice that pops up when you access the Internet or when you try to send a 5MB e-mail attachment to an external e-mail address; the message about call recording that you hear if you work in a customer services centre.

But what about the monitoring that develops over time? Something that didn't start out as monitoring but, five years down the line, has turned out to be a way of checking up on your members of staff? The temptation to use information that happens to be at hand may be too great to resist.

Phone monitoring

Virtually everyone who works for a living has access to a telephone at work. Whether it is a land line or a mobile phone, most employers need and want their employees to be able to talk to colleagues, clients, customers and suppliers. This, of course, generates phone bills, and these bills will be checked and verified for various reasons, the obvious one being that the employer does not want to pay for calls that are charged incorrectly.

A phone record can serve a number of useful purposes. It may provide a direct means of assessing compliance with an employer's policies. A record that shows one member of staff

spending three hours on the phone to an overseas number every day may indicate that this member of staff is ignoring a policy which prohibits excessive personal use of communications systems.

As well as checking for incorrect charges and misuse, the employer might want to check that their telecoms systems are being used efficiently. For example, those in the construction industry might start work on a site where there are no utilities in place. At this stage, the workers will have to rely on their mobile phones as a means of communication. However, after a few weeks, construction will commence, and site infrastructure will be installed. Once land lines have been connected, the employer will expect these facilities to be used as they are much cheaper than using mobile phones. The employer could use phone records to measure whether or not there has been an appropriate decrease in mobile phone usage by those working on the site.

An employer with staff working in a sales environment might use phone records to track productivity. This may be an issue for those working in call centre environments, where workers have efficiency targets and are measured on the number of calls and the speed with which they are answered, but it may also affect other employees. Senior executives in most industries are tasked with business development, in some cases this is a euphemism for cold calling. What better way to monitor how hard these executives are working than by checking the number of calls they make?

Access control systems

Sophisticated access control systems are frequently used in the workplace to allow authorised personnel to enter premises or a specific area within premises, and to prevent unauthorised access. The primary function of these systems is security. If the access control system is properly monitored, it will help to ensure that the employer's premises are accessed only by those who are entitled to enter. Monitoring may also be useful if a security incident has occurred, such as theft of items of computer equipment. The access control system may show who was in the office at the time of the theft and provide valuable information to the police.

This kind of use may be expected. But access control systems also reveal the whereabouts of members of staff, and this information may be useful to an employer for a variety of other reasons.

A manager who wishes to establish which member of his team is the most dedicated may find details from the access control system very useful. From this he can tell who arrives at work first and who leaves last. He can also see who spends a long time away from their desk having coffee or lunch and who is in the office with only a half hour break each day. On a more positive note, an employee who regularly spends an excessive number of hours in the office could be counselled about her work-life balance.

A manager in a rival team may also be interested in the access control details. This manager works on client-facing projects and her team charges the client for the time spent on a project. Team members are supposed to enter the details into the firm's timesheet system on a weekly basis, but they quite often forget or are too busy. The manager has to put together her billing details for the client project regardless of whether her team have entered their details, and so she uses the entry and exit times for each member of her team to calculate the number of hours worked. This proves to be such a foolproof method that she gives up on the timesheets and simply requests the entry and exit logs for her team members each week.

Rather like the combined credit and travel card, some employers combine their access control cards with payment cards for use in the office canteen. Not only can these employers control an employee's entry to and exit from the premises, but they can also record the time of day at which an employee uses his card to make purchases in the canteen. They could even record whether the employee is buying one of his "five-a-day" vegetables or fruit or has succumbed to chocolate. An employee whose performance in the afternoon seems sluggish could be steered towards healthy options in the office canteen.

They could even record whether the employee is buying one of his "five-a-day" vegetables or fruit or has succumbed to chocolate.

Expenses

A lot of publicity has been generated in recent months about MPs' travel expenses. Requests made under the FOIA led to the publication of these expenses, broken down into rail, road, air and bicycle use. This in turn led to press comparisons about the "greenness" of various MPs' modes of transport. The BBC news website reported that, overall, MPs spent about £2m on driving, £1.5m on trains and £1m on flights. Very few MPs made claims for bicycle use, with the highest individual claim being for £230, which equates to 1,150 miles by bike during the year. This information can clearly be used to rank MPs in order of eco-friendly travel and value for money, which might not give rise to a great deal of sympathy from taxpayers. However, it is not hard to imagine that other employers might use expense claim information in a similar way. If expense claims are assessed to check compliance with company policy, that is only to be expected, but if it results in the publication of green league tables in the office to encourage eco-competition between employees, that may not.

Why does this matter?

The Policy Studies Institute recently published a major research study on changes in the job conditions of the

British employees. The study, published by Oxford University Press on 6 December 2007, is entitled *Market, Class, and Employment* and was funded by the Economic and Social Research Council.

The research revealed that rising work strain is being caused by the use of information and communications technology to monitor and check work continuously. Controls over employees are intensifying, and surveillance using IT systems now covers more than half the workforce.

Some 52% of all British employees reported that a computerised system keeps a log or record of their work. Nearly one quarter said that this information is used to check their performance. This is confirmed by employers. At one in five workplaces, management claims that all employees are covered by computer-based monitoring systems.

The consequence of this has been a sharp increase in work strain for employees whose work is checked by IT systems compared with those in similar jobs who are controlled by more traditional methods.

Monitoring need not be a minefield

All of the above are examples of monitoring. Some may be carried out with the best interests of the employee at heart, but other forms of monitoring are clearly intrusive and excessive. How does one draw the line between monitoring that encourages effective working and compliance with company policy, and monitoring that places undue pressure on employees?

The Information Commissioner's Office has issued a detailed Code of Practice with a section specifically addressing monitoring. Part 3 of the Employment Practices Code makes it clear that monitoring is a recognised part of the employment relationship. Most employers will make some checks on the quality and quantity of work produced by their workers, and workers will generally expect this. However, where monitoring involves the recording and processing of personal data, it must be done in a way that is lawful and fair to workers. In broad terms, any adverse impact on workers must be justified by benefits to the employer and others. The code is designed to help employers decide whether this is the case by carrying out an impact assessment. If monitoring is justified, the code also makes it clear that workers should be aware of the nature and extent of monitoring and the purposes for which it is carried out.

Monitoring need not be a minefield; it simply requires thought on the part of the employer. The message seems to be that constant vigilance is needed to ensure that today's new technology does not become tomorrow's spy in the workplace.

AUTHOR

Valerie Taylor is a PL&B Consultant.

REFERENCES

1. www.psi.org.uk
2. www.psi.org.uk/news/pressrelease.asp?news_item_id=213
3. www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/employment_practices_code001.pdf.

Is there a person behind that IP address?

The Article 29 Data Protection Working Party Opinion that Internet Protocol (IP) addresses are personal data appears to have raised more questions than it answers. Nevertheless, companies that collect and process user IP addresses would be wise to reassess their privacy policies. **Dugie Standeford** reports.

The 4 April 2008 opinion, which specifically targeted privacy issues arising from search engine services, "raises the bar" on handling personal data, said Privacy International Director Simon Davies, a Visiting Fellow at the London School of Economics. Nevertheless, he said, the opinion's impact is unclear because of the "black hole" in knowledge about what companies actually do with personal information.

Search engines play two different roles with respect to personal data, the WP said. As service providers to users, they collect and process vast amounts of user data, including information gathered by technical means such as cookies. Data collected can range from the IP address of individual users, to extensive search histories, to information provided by users themselves when they sign up for personalised services.

The second role of search engines is as content providers who make Internet publications widely accessible worldwide, the WP said. In doing so, search engines regroup and republish data in "caches" that "create a new picture," with a much higher risk to the data subject than if each item of data were posted separately. "The representation and aggregation capabilities of search engines can significantly affect individuals... especially if the personal data in the search results are incorrect, incomplete or excessive," the WP said.

IP addresses, identifiable, numeric addresses that connect computers to the Internet, are among the types of information search engines process. A search engine may link different requests and search sessions originating from a single IP address, making it possible to track and correlate all logged Web searches launched from that address, the WP said. Internet service providers (ISP) increasingly assign fixed IP addresses to

individual users, and identification of a user can be improved if the IP address is correlated with a user unique identification cookie distributed by the search engine provider, since the cookie will not change if the IP address is modified, it said.

In its 20 June 2007 opinion on the concept of personal data, the WP clarified the situation by explaining that someone's search history is personal data if the individual to whom it relates is "identifiable." While IP addresses are generally not directly identifiable by search engines, identification is possible through a third party, such as an ISP, law enforcement authority, and, in some EU countries, a private party involved in civil litigation, the WP noted in its April opinion.

In most cases, including those where IP addresses are dynamic rather than fixed, "the necessary data will be available to identify the users(s) of the IP address," the WP said. It reiterated its earlier statement that unless an ISP can say with absolute certainty that data correspond to users who cannot be identified, it must treat all IP information as personal data to be on the safe side. The same considerations apply to search engines, the WP said.

A search engine, even one based outside the European Economic Area, that processes user data, including IP addresses, falls under the definition of a data controller because it effectively determines the purposes and means of the processing, the WP said. Search engines that function strictly as intermediaries are probably not data controllers, but those which also store complete parts of content on the Web, including personal information contained in the content, or offer value-added services linked to characteristics or types of personal data on the information they process, are.

The WP imposed several obligations on search engines. They include:

- Processing personal data for legitimate purposes only and ensuring the data are IP relevant and not excessive for the purposes for which they are being used.
- Deleting anonymised personal data when they are no longer necessary.
- Retaining personal data for no longer than six months.
- Giving users clear and intelligible information about their identity and location and the purposes for which they are collecting data.
- Obtaining user consent to retain individual search histories.

What is 'identifiable'?

The DP Directive applies to data relating to a natural person who is "identified" or "identifiable." In its 2007 opinion on the concept of personal data, the WP defined identified as "distinguishable" from all other members of the group, and "identifiable" as having the possibility of being identified.

> "Sweeping statements that IP addresses are always, or never, 'personal data,' are both wrong"

"Sweeping statements that IP addresses are always, or never, 'personal data,' are both wrong," Google Global Privacy Counsel Peter Fleischer said in an interview. It depends on the context, and in particular, whether an individual person can be identified behind the IP address. For most websites that is not the case, he said: There is generally more than one user per address; ISPs dynamically assign IP addresses so several different accounts may use the same address in the course of a week; and unless an IP address can be tied to someone's personal data, it can only be connected to a machine, not a human being.

Fleischer noted on his personal privacy blog the WP's position that the mere hypothetical possibility to single out a person is not enough to render him identifiable and to turn his IP address into personal data. Because IP addresses can move, and may be used by more than one person, the chance of Google being able to combine an IP address with other information held by a user's ISP to identify the individual is "negligible", he wrote.

Google, ad-serving service Phorm and others say, "It's just a number and we don't know who it is," so an IP address is not personal data, said Dr Chris Pounder, a privacy consultant and trainer at Pinsent Masons Solicitors. Information commissioners, however, argue that the companies are identifying individuals based on their characteristics rather than their names and must obtain consent to collect their information, he said. If the authors of the DP Directive had meant to restrict its application to people "identified by name" they would have said so, Pounder said, but instead they opted for the broader term "identifiable."

"If I were a betting man, I'd say it's right on the cusp," but that it leans toward IP addresses being personal data, Pounder said. There are circumstances, however, where that is not the case, he said. The UK Data Protection Act, for example, requires an analysis of the purpose for collecting personal data, and in some cases that purpose may not be linked to an individual. The context in which the information is to be used is key, he said.

Opinion's impact unclear...

Characterising IP addresses as personal data could have wide-ranging negative consequences, Fleischer said. Like most websites, Google collects IP addresses in order to monitor usage patterns and collect statistical information for security and quality purposes. Branding IP addresses personal data will hurt the search engine's technical operations, and hamper its ability to protect and serve its users.

The opinion also sets up compliance collisions with two requirements of the DP Directive, user consent and access and correction, Fleischer said. Google's only way of recording consent for unauthenticated users is by use of cookies. Moreover, all websites could be forced to seek consent each time a user's ISP changes the IP address assigned to that user's Internet device or whenever a user deletes cookies, he said. In addition, it is impractical for a website to give a particular "IP address" access, correction and deletion rights when it cannot identify the individual behind the address.

The opinion is a sea change in

attitude, said Davies. It declares that companies cannot assume to have the right, based on a business case, to use IP addresses as personal data. It reverses the default for online companies, which has shifted since the 1990s from opt-in to opt-out consent and toward the planting of cookies and use of IP addresses, he said. The problem is that there is a "vast black hole in our knowledge" about how search engines and other websites use personal data, so the effect of the Opinion is unclear, Davies said.

But 'every organisation is on notice'

Although the WP Opinion was limited to search engines, "IP addresses are used by every device and every website to direct data," Fleischer said. Any discussion of IP addresses in privacy terms is relevant to "every user, every device and every website on the Internet," he said.

The WP Opinion "puts every organisation on notice," Davies said. Any company that deals with IP addresses - search engines, ISPs, ad-serving services and the like - will have to review its data protection framework, he said.

Davies is a founder of 80/20 Thinking Ltd, which is preparing a privacy impact assessment for Phorm, the controversial ad-targeting site.

He tells PL&B that the consultancy is working with regulators to define how online consent can be achieved. He said the Working Group on Consumer Consent has the full support of the Irish, French, UK, Madrid, Slovenian and Berlin data protection commissioners. Many business models assume that opt-out is the only alternative, but Davies believes there are feasible opt-in mechanism as well. He expects the project to launch soon.

Companies spending millions of pounds on new information-collection technologies are not likely to want a definitive legal opinion on whether IP addresses are personal data, Pounder said. He predicted that the definition of identifiability will not be nailed down until some privacy commissioner pushes it. But ten years down the line, technology will be more precise and IP addresses will have to be treated as personal data, Pounder said.

AUTHOR

Dugie Standeford is a *PL&B* correspondent.

Children's privacy issues high up on EU agenda

The fact that an EU-level working party studies privacy issues affecting children indicates that the way companies process children's data will be under scrutiny in the future. **Laura Linkomies** explains what is at stake.

The body that is currently looking into how best to protect privacy of young people is the EU Data Protection Working Party. While its recommendations are not binding, they have an importance is shaping up the privacy agenda in Europe. Publishing a paper on the issue shows that the privacy commissioners aim to put more emphasis on these issues in the future.

The Working Party adopted, on 18 February 2008, a document that explains the DP Commissioners general concerns about data protection and privacy issues related to children. These are general guidelines, which fail to address specific questions, especially those in the commercial field. This is simply because the 27 Commissioners could not reach consensus on any of the tricky issues, such as how to gain a child's consent, how to verify it, and at what age children should be asked for their consent.

Speaking at the meeting of the PL&B Children's Privacy Protection Network in May, the President of the Portuguese Data Protection Authority, and one of the authors of the report, Dr Luis Novais Lingnau da Silveira, said that the group may return to the commercial issues in 2008-2009. Silveira explained that the paper was produced by a sub-group that consisted of 8-10 Commissioners. Even so, it was difficult to agree on certain issues. Silveira invited comments on this paper by 30 June 2008 and encouraged a dialogue between the sub-group and the PL&B group.

Consent and best interest

The Working Party's document reiterates that as the Data Protection Directive's scope is all natural persons, it also applies to children. According to the criteria in most relevant international instruments, a child is someone under the age of 18. But, there is no consensus on at which age children can give their consent, and verification would be extremely difficult, says Silveira.

The Working Group suggests that children should be treated in accordance with their level of maturity. This means that where consent is concerned, a child can, in some cases, give consent without any consultation with the guardian – say in order to subscribe to a free magazine – but parallel consent of the child and guardian is required for more elaborate processing, for example appearing on TV as a competition winner.

A similar approach was proposed at the PL&B meeting, looking at the general context where the child operates. Factors to look at would include the child's interaction with the service (to get an idea of age), what information is being collected, in which

jurisdiction (cultural differences play a part), how privacy-invasive a collection of data is, whether there is enough transparency, and what is the attitude of the DPA in that country.

Silveira explained that sometimes the best interest of the child can come into conflict with the requirement for consent from their guardians. "In Italy, the Data Protection Authority did not give permission to broadcast a programme where a very young child was talking about the problems in their family life. In this case the best interest of the child was seen as stronger than the parents' consent."

In Spain, a new regulation demands consent for the use of children's data. This is seen as extremely difficult to establish, even in the opinion of the Spanish DPA, which is advising companies to provide some evidence of age verification instead.

Silveira thought that there were some cultural differences across Europe but that these are mostly a mindset of adults rather than the children whose data we are trying to protect.

Privacy notices – specially written for children

An easy-to-apply privacy protection measure that can have immediate effect is a privacy notice. The EU Working Party recommends using layered notices, which are specifically written for children in a clear and understandable manner. Privacy notices should be posted at points of data collection and should include a link to a more detailed notice.

The Working Party stresses that privacy notices are an important tool in raising children's awareness of possible risks. All in all, the paper puts much emphasis on education. Schools are in the best position to address privacy issues, Silveira thought. Parents can do their share, but we should not rely on parents as they do not necessarily understand the threats connected with the online services the children use.

Schools

The Working Party addresses the field of education in particular. It says this area was chosen due to the importance of education in society. In the school context, there are various potential privacy problems. For example, student files are often created as early as when the children first enrol at a school. Any such forms should inform the children and their parents what purpose the data is being collected for, their right of access etc. In everyday school life, children's data is nowadays collected in terms of allowing access, for example to a school canteen, by using their biometric data. Other typical ways of collecting and processing personal data include running a school website, publishing statistics, taking school photos, monitoring children with CCTV cameras, gathering health data, etc.

The Working Party says that "data protection should be included systematically in school plans, according to the age of the pupils and the nature of the subjects taught".

Children should thus become autonomous citizens of the information society, and know their data protection rights.

INFORMATION

The Article 29 Working Party invites those who handle children's personal data, especially teachers and school authorities, as well as the general public, to comment on this Working Document. Comments should be sent to:
Article 29 Working Party - Secretariat - European Commission
Directorate-General Justice, Freedom and Security
Unit C.5 - Protection of personal data
Office: LX 46 06/80
B - 1049 Brussels
E-mail:
Amanda.joyce-vennard@ec.europa.eu
and
Kalliopi.Mathioudaki-Kotsomyti@ec.europa.eu;
Fax: +32-2-299 80 94

For more information about *PL&B*'s Children's Privacy Protection Network, and how to join, please see www.privacylaws.com/CPPN or e-mail Glenn@privacylaws.com

CONFERENCE REPORT

Northumbria Information Rights

By Helen Morris

The second Northumbria Information Rights conference took place on 1 May 2008 at the Gosforth Park Marriott, Newcastle Upon Tyne. Chaired by Helen Morris, who leads Northumbria University Law School's Masters programme in Information Rights Law and Practice, the conference featured an impressive line-up of speakers.

First up was Maurice Frankel, Director of the Campaign for Freedom of Information, who gave an overview of FOIA three years on. In general, it was a positive picture. Frankel commended Prime Minister Gordon Brown for his commitment to the principle of freedom of information despite the sometimes uncomfortable nature of the information released. He also pointed to the huge increase in public awareness of the Act, as shown for example by correspondence received by MPs from their constituents, who often demonstrated a much more detailed knowledge of the Act than the MPs themselves. On a less encouraging note, Frankel "named and shamed" some poor practice,

in particular from organisations which have adopted draconian destruction policies in order to avoid releasing information. This, he pointed out, is poor business practice quite apart from being wrong in principle. Finally, Frankel highlighted the difficulties caused by the continuing severe delays from the Information Commissioner's office.

2 Furthering Northumbria's strong links between the legal and information management aspects of the profession, Richard Blake, head of the Records Management Advisory Service at the National Archives, spoke about the role of the Records Management Code of Practice. He looked at the main changes in prospect under the revised code, including the extension of the types of records covered with more emphasis on e-mail, website services, and the new issues caused by collaborative working, home working and social networking. The new code is intended to be less prescriptive than the previous version, focussing on principles and outcomes rather than process level detail, and thus will give greater scope for different approaches.

3 Professor John Angel, chair of the Information Tribunal, then spoke on the developing role of the Information Tribunal. He looked both at the procedural issues, in particular how the Tribunal is coping with the volume of cases before it, and also at the range of important legal matters the Tribunal is addressing. Particularly welcome to delegates was the news that a search facility on the Tribunal website is on the way. John also talked about future directions for the Tribunal, including the possibility of it becoming an Upper Tribunal with precedent setting power following the ongoing review of Tribunal structures.

4 The Keynote speech was given by the Information Commissioner Richard Thomas, who among his many roles is a Visiting Professor in the Northumbria Law School. Thomas' speech entitled "Challenge and Change in the Information Environment" was wide-ranging. He talked about the "horrifying roll-call" of institutions admitting to "inexcusable security breaches" which had sounded a wake-up call to business and public sector to take information rights seriously, and had led to the numerous DP reviews currently in progress and to the prospect of reform. Thomas also looked at the benefits and the risks of information sharing, the ICO framework code of practice for sharing personal information and the use of privacy impact assessments. There is, he concluded, a "sea change in information rights", with FOI and DP cases setting the news agenda, and extensive Parliamentary and public discussion - and with universal awareness of the risks of getting things wrong, and the benefits of getting them right. Given the recent expansion of the Information Commissioner's powers to include issuing monetary penalties against data controllers who breach the data protection principles, it will be interesting to see how this approach is carried on into practice.

5 A panel discussion followed, covering among other things a request for advice from the panel about how to persuade unwilling bosses of the need to comply with FOIA. "Refer them to the growing list of Tribunal cases which name the individuals in public authorities who are personally responsible for non-compliance" was the strong message from the panel.

6 After lunch, Susan Wolf from the Law School spoke on Access to Environmental Information, and in particular the problems public authorities, the ICO and the Tribunal have had in correctly deciding whether a request falls within FOIA or the Environmental Information Regulations. She looked at why it is important to get this decision right, and examined the consequences of getting it wrong. Given that public authorities are still getting it wrong when it comes to the dividing line between FOIA and EIR, this talk was particularly timely.

7 Marcus Turle from Field Fisher Waterhouse gave a wide-ranging talk on data security, covering not only Data Protection but the many other legal and organisational issues that need to be considered in looking at data security and security breaches. His message was of the need for organisations to adopt a holistic approach based on the information life-cycle: the information life-cycle reveals the risk areas; the risk areas then reveal the legal considerations to be addressed; and the data protection principles represent the endpoint.

8 Last but not least, Tim Pitt-Payne of 11 Kings Bench Walk, who is also a Visiting Professor at Northumbria, spoke on Privacy in the Workplace. Tim looked at employer vetting of prospective employees, and asked whether the risk assessments made by prospective employers using "soft" intelligence raise problems for the privacy of individual potential employees. He also looked at the monitoring by employers of employees' phone calls and internet access, the issues around prospective employers accessing social networking sites, employees' blogging activities, and at the changing culture of the information world in which solutions to problematic areas may appear via technological developments and the increasing sophistication of users, rather than through legal controls.

The day finished with a further panel session which focussed on workplace issues and the effectiveness and enforceability of privacy policies in the workplace.

Before the panel, Andrew Watson, a member of the Northumbria Information Rights Team, took the opportunity to announce formally the launch of the Northumbria University *Information Rights Journal*, and to encourage delegates to submit articles for publication. The journal is looking for both academic articles and research and case studies from practice throughout the information rights sector.

Helen Morris
Programme Leader
LLM Information Rights Law and Practice
School of Law
Northumbria University
e-mail: Helen.morris@unn.ac.uk

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. E-mail 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 17.5% 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 ❑ E-mail ❑ Telephone

Name:

Position:

Organisation:

Address:

Postcode: Country:

Tel:

E-mail:

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, e-mail: sales@privacylaws.com web: www.privacylaws.com 09/06

www.privacylaws.com

Guarantee

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