ACTNOW

www.actnow.org.uk

May 2001

A Data Protection newsletter for the public sector

If you received this and don't want it email ActNow and we'll remove you from our mailing list. Please check the disclaimer, virus warning and copyright notice at the end of this newsletter.

In this issue

CCTV

Have you started worrying about giving subject access to your cctv systems? Did you see the Mark Thomas Comedy Product earlier in the year when he did a show on cctv and getting access to your own images? As well as being quite funny he did highlight how important it is for staff to know how to respond to a request for cctv footage. Following discussions with colleagues we've come to some conclusions. Firstly it's not as difficult as you think. Your cctv team will probably be able to isolate a time and a place quite easily. Secondly if an individual does request footage they have to supply you with a picture or you can't even start to search for their image. Thirdly if all the footage is long distance shots you can't identify third party images so you don't have to bother with masking peoples faces. The act says if you can identify people with other data in your possession - and for general street shots you don't have any other data in your possession. Starting point should be the code of practice prepared by the Office of the Information Commissioner (download it from her website)

DATA PROTECTION & CCTV

Data Compliance have been running training courses for CCTV system designers, managers and operators since early 1999. Hundreds of people have benefited from our expertise and knowledge as the leading independent specialists in CCTV and the law. Data Compliance has now produced this training course on CD Rom.
The first in a series of discs entitled "CCTV & the Law"; the Data Protection Act 1998 and CCTV will be launched in late April 2001. This product is designed to provide easily understood and practical interpretation of CCTV law.
The CD has 13 modules and provides all the essential information which CCTV owners; managers and operators need to comply with this legislation. Theoretical aspects of the law are fully explained by authors who know and understand the CCTV industry.

In particular, Local Authorities have many CCTV applications: Town Centres, Schools, Leisure Facilities, Council Offices, Housing tenant enforcement, Environmental Health etc. However, this training CD ROM has been written to cover all types of CCTV ownership, both public and private sector. This course is designed to train those who implement, manage or operate CCTV systems to help ensure full compliance with the law.
Data Compliance will update the CD annually and provide regular bulletins on our web site to help keep your use of CCTV legal. When you purchase and register your CD ROM, you will receive the first of these upgrades at a discount of 35%.
Data Compliance is pleased to offer this product to "Act Now" subscribers at a discount of price of £59.00 + VAT. (RRP £ 69.00 + VAT) This offer is valid until 30th June 2001.
Other Data Compliance services:
CCTV Manager and Operator training courses
CCTV Codes of Practice and Operational Procedures
CCTV system "Health Check" audits
CCTV Technical audits
To order this CD ROM:
Phone 01368 830727 Web www.datacompliance .com Email info@datacompliance.com
Fax 0870 132 8794

EMAIL POLICY

Readers will be aware from the last issues of ActNow that the Lawful business practice Regulations allows businesses to monitor their staff for relevant and justifiable specified business purposes provided they have made "all reasonable efforts to inform every person" who may use their system that e-mail or internet use may be intercepted. Law firm KLegal did a survey the findings of which suggests that one fifth of employers in the UK monitor the internet activities of their staff without informing them or gaining their consent.

The survey also found that downloading pornography was the main reason for sackings over misuse of internet and e-mail systems. One company in five said it monitors e-mails on a monthly basis while one in ten said it makes daily checks.
In a new survey of 100 business, entitled "Email: Coming out of the Amateur's Closet!" on behalf of Interliant, an ASP, people across various UK industries, 44% said they do not have policies in place for e-mail use by staff or have them but don't follow them.
The Information Commissioners Code of Practice on the use of personal data on the employer/employee relationship which also gives guidance on surveillance is now delayed. It was thought to be ready for final publication at Easter. It is now likely to be some months due to redrafting to take account of opposition from business who claim it is too strict and does not sit well with the above legislation.

For a full article on monitoring and surveillance in the light of recent legislation please go to our website www.actnow.org.uk

One item that's often argued about is the use of a disclaimer at the end of an email. One dedicated researcher has looked into the problem and you can see his results at Dundee Uni. There's also a link on this site to the worst disclaimers ever seen...

CRIMINAL RECORDS BUREAU

Check up on your staff before you employ them…
Sneaking in under section 56 of the Data Protection Act 1998 is a welcome but unheralded closing of a loophole. A person must not in connection with the recruitment of another person as an employee require that person to supply him with a relevant record. On the street it is known as enforced subject access. You may not have encountered it but if you

talk to any police Data Protection officer they will tell you that they receive thousands of such requests a year. Unscrupulous employers (are there any other kind) are requiring candidates for interview to obtain their police record (or evidence that they don't have a police record) and bring it to the interview. The employer cannot obtain this as data protection law forbids it but they can say to their potential employee that if they don't make this subject access request and hand over the result they needn't bother turning up for the interview. I have even know employers who have asked for the envelope to be given to them unopened! Section 56 puts a stop to this.

The margin note says 'Prohibition of requirement as to the production of certain records'. So apart from the police suddenly having a significant drop in the number of subject access requests (just in time to re-deploy the staff to Freedom of Information requests) what effect will it have on employers? Will they be able to check up on their potential employees criminal past? The answer is yes.

The Criminal Records Bureau is being set up in their own words 'to help organisations make safer recruitment decisions'. Employers will be able to perform their own check on their future employees if the work involves children or vulnerable people or some other categories such as List 99 - a Dfee list of people barred from working in schools. Based in Liverpool it's a joint venture between Home Office and Capita that will eventually employ a thousand staff. The method of operation is quite simple and the costs involved are reasonable. Employers wishing to take advantage of the system have to register at a cost of £300 and each disclosure of information about an individual is £12. Employers have to abide by a code of practice drawn up by the CRB to ensure the information is handled fairly and they are also required to have a policy in place over recruitment of ex offenders. Registration will start in May this year and the first disclosures will be sent out later in the year.

There will be different levels of disclosure. The first is a Standard Disclosure for positions that involve regular contact with children or vulnerable adults. They may also be relevant for people in positions of trust. This disclosure will contain details of all convictions on record including current and spent convictions (bearing in mind that most convictions are never spent) and they include details of any cautions, reprimands or warnings held by the police. It may also have information held on government department lists of those unsuitable to work with children or vulnerable adults. The other type of disclosure is an enhanced disclosure. As the name suggests these are for posts involving greater contact with children or vulnerable adults, being in sole charge of such people. These may also contain information that is held locally by the police; what we might call intelligence.
How do I find out more or how does my organisation register to use the Criminal Records Bureau? There are several ways.

Firstly start with the website and there's plenty of information there. Call the information line on 0870 90 90 811 or they are also organising a series of day long seminars. These are well spread about the country so during May and June you can go along and listen to the Bureau. These are free and include lunch! What more could you want? It's crucial that this is managed at a corporate level. The last thing you want is many people within your organisation deciding to register themselves. Maybe you could put this into your Information Management function...

NEED ASSISTANCE WITH RECORDS MANAGEMENT?
Readers will now be aware that with the Data Protection Act and Freedom of Information Act organisations will need instant access to critical information, every time, on time? This

is easier said than done. Paper documents take up space and can easily become disorganised, whilst digital documents are often buried within huge servers, or aren't accessible from different types of computers.
Cave Tab is a company which helps organisations like Local Authorities, Housing Associations and Health Trusts manage information and use it more efficiently. Cave Tab offers solutions for managing information from paper to electronic documents and beyond. Cave Tab will develop a customised solution that's right for your needs, whether a single department or an entire organisation. Cave Tab will develop a formal proposal, outline a set of processes and help you choose the products that help your enterprise store, manage and use information more effectively than ever before.
Cave Tab products and services incorporate:
File Tracking Software, High Density Storage Solutions, Colour coded indexing software, Document Imaging Software, Specialist Archive Services, Project Management, Records Management Consultancy Services, Audits and Advice
For more information Call 0800 616347 or visit Cave Tab.

CAUTIONARY TALES

This comes from an item on a national bulletin board where subscribers were asked to contribute funny stories to illustrate data protection concepts.

I came from the police arena and I have a "horror" story the first involves a police officer checking the PNC (Police National Computer) for the registration of a vehicle, because the lady he was chatting up in a club drove off in it and he wanted to contact her. She complained about misuse of his power to track her, (she obviously was not as impressed by him as he with her!), the officer was disciplined and was reduced in rank!!

I know of a very recent case where a large utility was opening up a call centre, the trainees were given the live system to practice on, and given free rein to look up accounts of anyone they knew. So much for data protection!

A friend of mine works for a company that has a telephone answering system which identifies the caller and brings up their details on a pc in front of the telephone operator to help them answer the caller's enquiry. The system is also capable of displaying an automatic "warning screen" on the pc if there is anything significant about the account. After one long and tiresome session with a particular caller, an operator decided to create a "pop up" warning that said "Be very cautious in your approach to this customer".
The operator was not wholly familiar with the computer system, and, unfortunately, rather than create a warning notice screen, the address screen of the caller was actually changed. The matter was drawn to my friend's attention by the (even more irate) caller who was astonished to find the offending text inserted between their name and address when the next bill was delivered...

Only the variant of the one you describe, which I think I circulated as a"cautionary tale" last year. Policeman called us with information about an alleged assault on one of our students and asked for home address. Gave us the phone number of his police station in Devon so that we could call back to verify his credentials. We called back and a person in a Devon accent put us through the switchboard to their personnel office who verified the identity, ID number etc of the caller. So we passed on the information. Turned out that this phone number was a callbox on the moors somewhere, and the all the parts were played by the original caller - himself, switchboard, personnel officer, clicks on the line during transfer etc. We only discovered this after the student complained about unsolicited calls from a

harasser. Moral: check directory enquiries (or your local police) to verify the phone number of the police station too!

A real incident occurred here early last year that incurred the wrath of the Registrar/Commissioner. One Department holds regular sickness monitoring meeting. At these meetings, various reports and sickness records are discussed, including some personal sickness reports. At one meeting, it was discovered that the statistical analysis was wrong, being based on incorrect data. The Personnel Manager immediately agreed to re-circulate the right information. She issues an instruction to one of her subordinates to send them out "urgently". This was done but to save time, the whole data set was corrected and sent out - just with a compliments slip but without an envelope! A union rep spotted this. Rather than simply take up the matter directly with the Personnel Manager, he wrote to Wilmslow. An official investigation was called and the Department had no option but to plead guilty. Confidential and personal information should have been circulated in sealed envelopes and marked for the attention of the addressee only. The Department was forced to review procedures and carry out some DP training

One thing of a "good awareness" variety I noticed recently in a hospital in New York was a sign in each elevator that said,"Staff are reminded that patient records are confidential and should not be discussed in public places, including the elevator." The opposite of that is the story told by the former Data Protection Commissioner of British Columbia, Canada, who visited a hospital and found patient records piled next to the registration office at the front door to the hospital where everyone entered the hospital and could easily pick up and read, or even walk off with, a record.

A large, well-known firm of loss adjusters investigating an insurance claim sent a form to a London borough informing them that they were under a statutory duty to tell the company whether the individual was paying council tax and if they were resident at a particular address.

Virgin Atlantic Airlines sent a letter to a passenger which began "following the flight of you and your wife" - he was travelling with his secretary!

A school teacher told me that every night before they went home the last person in the school office dutifully crawled under the table and pulled the phone line out of the wall 'so that no nasty viruses could get into school and no-one could steal their data during the night'. First person in school in the morning put the internet back on!

Funny Stories always welcome... It's hard enough delivering training and these do help. Here's 3 real life ones.

A police clerk, has been fined £3,000 by Llanelli Magistrates Court for illegally using the Police National Computer. The purpose was to check up on her 13 year old daughter's 19 year old boyfriend of whom she disapproved.

B&Q in Bournemouth employed a teenager as a salesman and within a week had considered him for promotion to weekend supervisor as he worked so well. But when the results came through of an automated personality test taken before he started work he was sacked for failing the assessment.

The Labour Leader of Bromsgrove Council was recently convicted of an offence under the Data Protection Act. He obtained information illegally and used it for political advantage more details

DATAEDGE

Are you still struggling with your policies and procedures to comply with the Act? Help is available in the form of the DataEdge compliance tool kit. It has been produced by Hammond Suddards Edge a firm of solicitors with offices throughout the country (website). The kits are ideal for any organisation which wants a ready resource upon which to base a data protection compliance programme. Each kit contains very useful material such as a data protection policy, data processor agreement, security checklists and employment contract clauses. They are available for sale at the reduced rate for local authorities of £500 (no vat). The normal price is £750. Anyone interested should contact Hammond Suddards Edge on 0121 2002001 or email Caroline Egan

GEORGE BUSH WRITES A LETTER

Want to know what George W Bush thinks of Data Protection laws? In a letter to the European Union dated March 23rd, the Bush administration took issue with the burden that European privacy rules would place on U.S. financial institutions. The letter called the EU rules "incompatible with real-world operations." Proposed standard clauses for contracts that govern the transfer of data from EU firms to companies in the U.S. are the chief concern, said the letter to the EU's e-commerce commissioner John Moog. The European Parliament must still approve the standard clauses but they are expected to become effective this summer. The letter asks the EU to delay implementing the standard clause rules. As an example, the model contracts would require U.S. firms to notify European consumers how their personal information is used and to give European consumers access to personal information that has been collected about them. The EU privacy law would require U.S. companies to apply EU law in the United States for European consumers, which the U.S. believes infringes upon its sovereignty. For more on how the americans view our Data Protection regime look at the US Department of Commerce

CATHERINE ZETA JONES

Who said data protection is boring? Which of your colleagues can mention Catherine Zeta Jones in a serious conversation about their work area? Read on! All will be revealed!

The Human Rights Act came into force on 2nd October 2000. It means that the European Convention on Human Rights is now part of our law. One of the Articles in the Convention is the right to respect for private and family life (art 8). Those who have attended our courses will know that this extends to the use and disclosure of information about individuals. But to what extent does this give an individual the right to privacy? Just months into the Human Rights Act, the first law of privacy is already being carved out in the courts. In Michael Douglas, Catherine Zeta-Jones and Northern & Shell Plc V Hello! Ltd (2000), Michael Douglas and Catherine Zeta-Jones won backing for claiming a right to privacy over the unauthorised use of photographs by Hello magazine.
Hello claimed that Freedom of Expression set out in Article 10 of the European Convention on Human Rights gave them the right to make public comment, including publishing the photos. The Douglas's claimed they had a right to privacy, which had been invaded under Article 8.

Lord Justice Sedley stated that "we have reached a point at which it can be said with confidence that the law recognises and will appropriately protect a right of personal privacy. The reasons are twofold. First, equity and the common law are today in a position to respond to an increasingly invasive social environment by affirming that everybody has a right to some private space. Secondly, and in any event, the Human Rights Act 1998 requires the courts of this country to give appropriate effect to the right to respect for private and family life set out in Article 8." In addition, he commented on the balance between the rights to privacy and free expression, stating "the reputations and rights of others - not only but not least their Convention rights - are as material as the defendant's right of free expression."
This case is very important because for the first time the courts have recognised that there is a right of privacy in the UK courts which will be protected by the courts. It serves as a reminder especially to the public sector that they must bear in mind this right in all their actions and decisions. This is especially so with regard to the processing of personal data and adherence to the Data Protection Act 1998

FREE DOWNLOAD
DJ Freeman solicitors have produced a guide to the Human Rights Act 1998. This can be downloaded from their website or from their marketing department (email) in hard copy or a mini CD. It is an extremely useful introduction to the Act and the CD may assist as part of a training programme.

FREE E-GOVERNMENT NEWSLETTER
E-Government Bulletin is the first and best free email service covering electronic public services, 'teledemocracy' and the information society in the UK and worldwide. The Bulletin is an independent publication, aimed at everyone in government, local government, the social sector and their private sector partners. It is absolutely free to receive, subscribers are free to unsubscribe themselves at any time and as registered Data Controllers we never pass on email addresses to third parties.

Issues covered in the bulletin include how freedom of information and data protection law affect public bodies in the information age.

To receive a free regular copy, simply email e-government bulletin with a blank email and follow the instructions on the confirmation email you will receive. Please circulate the Bulletin to all your friends and colleagues - the more subscribers there are, the better this free service can become. For further information see Headstar's website

THE SOCIAL SECURITY FRAUD BILL and other forthcoming legislation
This Bill was introduced in the House of Lords on 18th December 2000. It seeks to implement one of the recommendations of a recent that the Government should examine how to make use of information held by the private sector to tackle benefit fraud. The Bill gives additional powers to those investigating benefit fraud and errors to obtain information from specified private and public sector organisations.

The measures in the Bill amend and build upon current legislation in sections 109B and 110A of the Social Security Administration Act 1992 These provide for authorised officers to obtain information in relation to employment and pensions. The measures in the Bill will provide for these officers to require information about individuals from specified private (e.g.banks) and public sector organisations. Information may be obtained where it is reasonable for the purposes set out at section 109A(2) and 110A(2), and where it is legitimate to make an enquiry about the person concerned. The list of specified private and

public sector organisations that can be required to provide information can be extended by an order in Parliament.

Utilities: The measures also provide for specifically authorised officers to require general information from utility companies about the quantity of services supplied to residential properties. The DSS intends to match this information electronically with benefit records in order to detect fraud. For example, if a person was claiming Income Support at a particular address and was consuming no electricity at that address this could indicate that he does not, in fact, live there and that his claim may be fraudulent. The measures do not provide for the bulk acquisition of individuals' names, only details of utilities supplied to residential addresses.

Penalties: If those from whom information has been requested fail to comply with authorised officers' requests they can be prosecuted under the current section 111 of the Social Security Administration Act 1992. They may be fined up to £1,000 plus £40 for each day after this that they continue to fail to provide the information requested.

Electronic Access: Clause 2 of the Bill provides that the Secretary of State and authorities administering Housing Benefit or Council Tax Benefit can require organisations to enter into arrangements so that the information can be provided electronically on-line where facilities exist to provide such access. For example, credit reference agencies provide direct on-line access to their databases instead of processing enquiries in writing. The clause provides that only those officers especially authorised can use such on-line facilities. This clause enables the Secretary of State and authorities administering Housing Benefit or Council Tax Benefit to require the provision of audit trail information in the arrangements in order to ensure that officers' use of the system can be thoroughly monitored. Authorities administering Housing Benefit or Council Tax Benefit are prevented from requiring an organisation to provide on-line facilities without the consent of the Secretary of State. They are also prevented from entering into a voluntary arrangement for on-line access to private information without the Secretary of State's consent.

It is clear that this Bill will assist central and local government in the fight against benefit fraud. However one has to question the need for such wide powers to request information form all sorts of bodies especially where section 29 of the Data Protection Act already allows organisations to disclose information where a criminal offence e.g. benefit fraud has been committed. It will be interesting to hear the comments of the information commissioner and civil liberties groups as the bill makes its way through Parliament.
Vehicle Crimes Bill
Clause 36 of this Bill will enable the police to have bulk access to an insurance industry database which will help them to detect people driving without insurance. In fact this seems to be part of an assault on motoring offences. In December last year it was announced that the Government has authorised the installation of cameras along roads to photograph the number plates and tax discs of passing cars, whether they are committing a crime or not. This will then be checked by the DVLA to detect and deter road tax dodgers

The Health and Social Care Bill
This entered the Commons in February. Under clause 59 the Health Secretary has the right to "disclose and process" even confidential patient information. The declared purpose of this Clause, according to the explanatory notes which accompany it, is to: "enable the Secretary of State to require or permit patient information to be shared between organisations for medical purposes where he considers that this is in the interests of improving patient care or in the public interest." The Bill has been widely slated by the Civil

liberties groups as well as the British Computer Society (website) which has issued a statement in response to it.

Animal Rights and Companies House
Animal rights activists have targeted recently directors and employees of Huntingdon Life Sciences (HLS) the animal testing facility. Brian Cass, managing director of HLS, was attacked outside his home by three masked assailants carrying baseball bats. As part of their campaign they obtained the residential addresses of various directors from Companies House.

All directors must file their usual residential address at Companies House whose Companies Register is available for inspection by anyone. The targeting of companies and individuals and their data by activists and, in the past, by terrorist groups, brings into question the public availability of such data.
The Government has introduced a clause in the Criminal Justice and Police Bill that will give protection to directors at genuine risk of violence by keeping private their home addresses. Under the amendment, a home address would still have to be provided but it will be kept on a separate, secure register available only to organisations such as the police.

The Information Commissioner commissioned a report into the sources and uses of publicly available data (www.dataprotection.gov.uk) and it will be interesting to see whether any further restrictions on public data will be introduced.

USEFUL BOOKS

The British Computer Society has produced a couple of very good books. One is entitled "Data protection - Everybody's Business" . This explains the new Act in depth. The other is called Data protection - Implementing the legislation." This gives sound advice on practical measure. Both are available from the BCS website : www.bcs.org.uk or phone : 01793 417417. Please mention ActNow and you will get a £5 discount

ACT NOW - DATA PROTECTION TRAINING FOR THE PUBLIC SECTOR
So far 86% of delegates at our seminars who completed a feedback sheet have rated them good or excellent. Consequently we have received many requests to present the course in house. We have now improved it to incorporate FOI, HRA and RIP. If you would like us to deliver training to your organisation please contact us. Organisations in an area may wish to club together so that they can share the costs and resources. Our availability is limited therefore the sooner you contact us the better. See our website for details.

Our free new website

Please visit our new website **ACTNOW.ORG.UK** As well as information on our courses you can get free information on how to stop junk mail/phones and faxes. You can also download free articles on relevant topics in this area e.g. surveillance and monitoring, freedom of information act and information management. There are also lists of resources and other useful downloads. You can also write individually to Paul Simpkins or Ibrahim Hasan. Next newsletter Sept 2001