Welcome to the July 2003 issue of the Act Now Newsletter on Data Protection, Freedom of Information, privacy and information management issues in the Public Sector. With over 1,250 subscribers we are undoubtedly the most popular newsletter on this subject in the UK.

This is a text version of the newsletter. You can read a HTML version online at www.paulsimpkins.btinternet.co.uk/JULANNL.htm

If you've received this from a colleague you can subscribe in your own right by logging on to www.actnow.org.uk and choosing Newsletter from the menu. You can also unsubscribe on the same page.

Please read the disclaimer and other important information at the foot of the newsletter.

****

In this issue

****

Course it's not just a newsletter

During the first half of 2003 Act Now also offered a series of 8 seminars/workshops on issues such as Data Protection, Freedom of Information, Records Management and Surveillance law at venues around the UK. Guest speakers included Rosemary Jay, Shelagh Gaskill, Philip Jones and Bernadette Livesey. These courses were extremely very well received. The average number of delegates was 24 per course and feedback was generally very complimentary. The Autumn programme offers a similar series of courses at regional venues at still only 145 pounds per delegate. This is substantially lower than many other training providers. Look at www.actnowtraining.co.uk for this autumn's programme. There are courses at

Manchester, Belfast, York, London on DP, FOI, RM and RIPA

And for those thinking how e-gov will affect their organisations in the area of booking courses of 196 applications received 51% used the fax to book, 31% used the online booking form, 9% phoned and 9% wrote enclosing a purchase order. Most of the organisations paid by cheque but half way through the programme organisations started requesting payment by BACS details. Of the last 50 invoices sent 32 used BACS to pay.

****

Connexions Service

Thanks to Martin Gibson (Bucks) who posted this on the NADPO website and gave permission for us to reprint it here.

The Department for Education & Science's view on the legality of the transfer of information from schools and LEAs to the Connexions Service and the Connexions Card is as follows

Legal Basis

Section 114 of the Learning and Skills Act 2000 (LSA) provides the basis of the establishment of the Connexions Service, in that the Connexions Service aims to support and encourage effective participation by young persons in education or training

Under section 117 LSA, if the Connexions Service request information about a pupil, the school have to pass that information to the Connexions Service. This provision is not dependent on consent. However, a school should not pass information (other than the name and address of a pupil or student and a parent of any pupil or student) if a parent of a pupil under 16, or a pupil age 16 and over has instructed the school that this information should not be provided. In all other cases, schools will be under a duty to pass on the information on request. In all cases, schools will be required to pass the name and address of a pupil or student and the name and address of a parent of any pupil or student, if requested by the Connexions Service to do so
If school does not pass this information to the Connexions Service, when requested to do so, the school will be in breach of its statutory duty

Under section 120 LSA, a local authority has the power to supply information about a young person to the Connexions Service, for the purpose of the provision of services in pursuance of section 114(1) LSA ("services which [the Secretary of State] thinks will encourage, enable or assist (directly or indirectly) effective participation by young persons in education or training")

Data Protection Act

Whilst all Principles in the Data Protection Act 1998 (DPA) are equally important, the First Principle is often considered the most difficult to satisfy the First Principle is that personal data must be processed fairly and lawfully and, in particular, must not be processed unless-
(a) at least one of the conditions in Schedule 2 is met, and
in the case of sensitive personal data, at least on of the conditions in Schedule 3 is also met
"fairly"

Making 'fair processing information' readily available to pupils/parents (as required by Schedule 1 Part II) is only part of the general "fairness" requirement. However, schools and LEAs as data controllers, should be able to meet these fair processing requirements, by schools sending out the suggested text (which was sent to LEAs along with guidance last month). It is envisaged that the Connexions Partnerships (through whom the Connexions Service is delivered) will provide to the pupils/parents, fair processing information explaining the purposes for which the pupils'/parents' data will be processed and any other further information considered necessary

"lawfully"
As mentioned above, S117 LSA provides the lawful basis for the transfer of information from schools to the Connexions Service and S120 LSA provides the lawful basis of the transfer of information from local authorities to the Connexions Service

Schedule 2 and Schedule 3 Conditions
Consent of the pupils or parents is not required for this transfer of information because other conditions in Schedule 2 and Schedule 3 are met
Other relevant conditions are:
Schedule 2
- The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract. (paragraph 3) [this applies to schools]
- The processing is necessary-
(a) for the administration of justice,
(b) for the exercise of any functions conferred on any person by or under any enactment,

(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or
(d) for the exercise of any other functions of a public nature exercised in the public interest by any person.
(paragraph 5) [this applies to schools and LEAs]
Schedule 3
- The processing is necessary-
(a) for the administration of justice,
(b) for the exercise of any functions conferred on any person by or under an enactment, or
(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.
(paragraph 7) [this applies to schools and LEAs]

Connexions Card

Legal Basis

The Connexions Card is an initiative which has the aim of encouraging young persons to stay in learning at 16. It is a service which the Secretary of State has the power to secure under s114 LSA. The Connexions Card is separate from the Connexions Service, but both are mutually supportive, helping to deliver each other's objectives.
As with the Connexions Service, s117 LSA provides the legal basis for schools passing information to those delivering the Connexions Card and s120 LSA provides the legal basis for local authorities passing information to those running the Connexions Card.
The same statutory obligations on schools as those set out above in relation to the Connexions Service apply to the Connexions Card.

Data Protection Act

The First Principle

"fairly"

The Connexions Card is an entirely voluntary scheme. A young person does not have to have a Connexions Card if he or she does not want one. A Privacy Statement is distributed to all young people when they register as card members which informs them of the purposes for which their data is being processed, who their data may be shared with and other relevant information. The Privacy Statement allows the young people to choose whether or not they are content for data about them to be passed to other organisations. This "fair processing information" is also contained on the Connexions Card website (connexionscard.com)

Where information on young people is passed from schools to those delivering the Connexions Card, the school is explicitly requested to inform pupils prior to passing the information that they are going to do so. Schools are also requested to give the pupils the chance to refuse the information being passed

"lawfully"

As with the Connexions Service, s117 LSA provides the lawful basis of the transfer of information from schools to those delivering the Connexions Card and s120 LSA provides the legal basis of the transfer of information from local authorities to the Connexions Service

Schedule 2 and 3 Conditions

Those relevant to the transfer of information from schools/LEAs to those delivering the Connexions Card will be the same as those mentioned above in relation to the Connexions Service. In terms of the processing carried out by those delivering the Connexions Card, consent for this processing is obtained from the pupils when they register for a Card.

Summary of a Legal Opinion obtained on the legality of Connexions request for data.

1. Disclosures of any personal data other than the names and addresses of pupils and parents could amount to a breach of

a) the Data Protection Act and/or

b) Article 8 of the Human Rights Act

2. Section 117 (1) (a) and (b) of the Learning and Skills Act allow for the transfer of names and addresses without the permission of the parents or pupils.

3. The Connexions service has claimed an exemption from the 1st Data Protection Principle by virtue of legislation. This Principle states that you need consent of the data subject to process the data. The Connexions service is claiming an exemption because the processing is 'necessary' by virtue of an enactment.

The legal opinion questions the premise that the Connexions service has demonstrated that the processing is 'necessary'.

4. The draft 'Fair Processing Note' from Connexions which they advise should be sent to pupils/parents, does not contain sufficient information to allow pupils or parents to properly exercise their right to opt out of the transfer of any data other than their names and addresses

5. The draft 'Fair Processing Note' could be confusing to pupils and parents because it doesn't make clear who the data controller is. In other words is the process being run by the school, LEA or by the Connexions service?

6. The draft letter fails to explain to pupils or parents the range of data likely to be sought making it difficult for the pupils or parents to know what they are opting out from. The letter also fails to explain whether an opt out can be applied later.

7. Because the opt out has not been adequately explained, this appears to be a breach of the 1st Principle.

8. In situations where schools intend to use the Connexions Card to monitor attendance, this would make cards compulsory in those schools and would appear to be a breach of the 1st Principle.

View from a Parent of a 15 year old student

I haven't heard a single thing from the school my child attends regarding the transfer of his data or my data to Connexions (and I know about the issue!!)

The Privacy statement of Connexion website.

http://www.connexionscard.com/x/c/cxc.jsp?P1=PRPO A good attempt but some questionable statements. Elsewhere Connexions claims to have 5,200 discounts on offer. That's 5,200 places that have your personal data including your views & interests!

The application form

https://www.connexionscard.com/connexionsImages/NonPersonalisedApplicationForm.pdf

The old chestnut about "organisations whose products we think will interest you" – as if young people can't think for themselves.

****

Website re-design

Act Now has changed the look of the website. It's now faster to load and cleaner and we hope easier to navigate. Look at www.actnow.org.uk to see if you think it works.

****

Requests under Freedom of Information

In the quest for information on the 30th May an Act Now researcher recently made 3 requests quoting Freedom of Information to Central Government, Local Government and a Town Council.

The questions asked were a)

Town Clerk
A Town Council

Dear Sir or Madam:

I write for information under the Freedom of Information Act 2000. Please could you tell me how many of your Town Councillors, since the institution of your Town Council, have

been elected in a contested election
been elected unopposed
have been co-opted.

Could you also tell me how many of your Town Councillors have received any expenses, the amount of those expenses and the reason for the expenses.

I look forward to your reply. As I am sure you are aware the Act allows 20 working days for you to respond in full.

b) To a local Education authority

Chief Education Officer
********* Council

Dear Sir or Madam:

I write for information under the Freedom of Information Act 2000.

Please could you tell me the salary paid to the Headteacher, Deputy Head Teacher, Acting Head Teacher and Acting Deputy Head Teacher of ****** School starting when the two schools were merged to create one school up to the present day.

I look forward to your reply. As I am sure you are aware the Act allows 20 working days for you to respond in full.

Yours faithfully

The Lord Chancellors Department

FOI Officer
Lord Chancellors Dept
Selborne House
54-60 Victoria Street
London
SW1E 6QW

Dear Sir or Madam:

I write for information under the Freedom of Information Act 2000.

Please could you tell me the names and job titles of the persons appointed to the Information Tribunal in 2002 and 2003. Could you also supply details of the experience of tribunal members in Data Protection and Freedom of Information issues such as possession of qualifications, previous teaching/training/lecturing on

the subject, conference speeches, papers published, chairs or professorships held. membership of relevant professional bodies.

I look forward to your reply. As I am sure you are aware the Act allows 20 working days for you to respond in full.

Yours faithfully

To see the responses click on www.actnow.org.uk and articles. Before you do you might like to consider what you would do if you received such a request. Not everyone will wait until January 2005. Act Now is running a FOI course in Manchester on November 5th.

****

LACORS CT and IR

The Local Authority co-ordinators of Regulatory Services (www.lacors.gov.uk) have been working on a memorandum of understanding for exchange of data between Local Authorities and the Inland Revenue. Here's the Introduction.

The Inland Revenue and the law enforcement agencies recognise the value of clearly identifying the legislative, policy and practical implications of disclosing information.

It is essential that the Inland Revenue and law enforcement agencies embrace the principles set out in this document. It is the duty of the Inland Revenue to maintain the confidence in which customers provide the department with information whilst at the same time co-operating with law enforcement agencies where internal Inland Revenue policy and the law allows it.

The Anti-Terrorism, Crime and Security Act 2001 came into force on 14 December 2001 and is supported by a Code of Practice. The Act introduced provisions that enable the Inland Revenue to disclose information to law enforcement agencies for the purposes of assisting criminal investigations and proceedings

This Memorandum of Understanding builds on the principles regarding the disclosure of personal information by the Inland Revenue to law enforcement agencies as described in the Code of Practice. Information will be disclosed by the Inland Revenue only to law enforcement agencies that agree to abide by the principles outlined in the Code of Practice.

PURPOSE OF THE MEMORANDUM OF UNDERSTANDING
The purpose of the Memorandum of Understanding is to document the arrangements and obligations when Inland Revenue provide information to a law enforcement agency.

Whilst the Act does not make mandatory the disclosure of information, providing that a request from a law enforcement agency follows the guidance set out in this document, the Inland Revenue will normally disclose the requested information.

Looks interesting? There are 16 more pages of it and the result is an information sharing protocol between Local Authorities and the Inland Revenue. To find out more log on to the LACORS site (ask you environmental team for the password) and decide whether you think this gives you powers to share information. Apparently 80 Local Authorities have already signed up although I also know of some who don't think it cuts the mustard.

****

More on Information Tribunal

Following an advert in the Guardian over a year ago over 170 people applied for the position of lay member of this tribunal. Half were interviewed and 8 were appointed. They were

Dr Malcolm John Clarke (56) is self employed, with his own consultancy acting as a facilitator and trainer in the public and voluntary sectors. He is an arbitrator for ACAS and also a lay member of the General Social

Care Council.

Mrs Suzanne Marie Cosgrave (47) is Operations Director for International Tax Services (Ernst & Young, London), and also a member of the town council of Burgess Hill.

Peter John Bellett Dixon (57) is Chairman of the University College London Hospitals NHS Trust and a board member of London & Quadrant Housing Trust and Anglia Housing Group. He is also Treasurer of the Naval Dockyards Society.

Dr Henry Antonie Fitzhugh (58) is retired Director of marketing & development for the Royal Horticultural Society. He also excelled in his profession as a scientist.

John Paul Randall (55) is a self employed consultant advising and training on Higher Education accreditation and quality. He is a member of the Council of the City & Guilds of London Institute and as lay member for the College of Personal Injury Lawyers.

Anthony David Stoller (55) is Chief Executive for Radio Authority. He also sits on the committee of Reference for the Friends Provident Stewardship Ethical Fund.

Mrs Jennifer Anne Thomson (61) is the Founder and Director of the Gaia Trust, which specialises in education and sustainable development. She also chairs the South West Environmental Protection Group and the Eastern Europe Development Association.

Ian Patrick Wilson (61) is retired Interim Chief Executive for a Policing Board. He has held many senior posts including Treasury and Cabinet Office Under Secretary, a Director of the Central Computers and Telecommunications Agency and Executive Advisor on finance
initiatives projects for International Computers Limited.

Clearly an in depth knowledge of Data Protection and Freedom of Information was not necessarily required for the appointments. Whether this is a good or a bad thing is open to debate but none of these appointments are known in the sector at all.

****

A message from Bill Gates (whoever he is…)

June 24, 2003

Email is such an integral part of business and everyday life today that we tend to forget how recently it became popular. The first email program was developed in the early 1970s, but for two decades the technology was hardly used - except by computer scientists, researchers and hobbyists.

Not until the mid-1990s, when the growing popularity of personal computers converged with easy access to the Internet, did email become truly pervasive as a way to communicate at work, with family and with friends. Today, email is as easy to use as the telephone, and just as vital for keeping people in touch, and for improving business productivity.

Yet email's popularity has produced one very troubling side effect: spam. Unsolicited commercial email is a spreading plague that feeds off the unique power of the Internet to connect hundreds of millions of computer users around the world, at virtually no cost. Generally unwanted - and often pornographic or with fraudulent intent - spam is a nuisance and a distraction. Like almost everyone, I receive a lot of spam every day, much of it offering to help me get out of debt or get rich quick. It's ridiculous. What's more, spam is a drain on productivity, an increasingly costly waste of time and resources for Internet service providers and for businesses large and small. It clogs corporate networks, and is sometimes a vehicle for viruses that can cause serious damage.

Spammers often prey on less sophisticated email users, including children, which can threaten their privacy and personal security. And as everyone struggles to sift spam out of their inboxes, valid messages are sometimes overlooked or deleted, which makes email less reliable as a channel for communication and

legitimate e-commerce. Spam is so significant a problem that it threatens to undo much of the good that email has achieved.
At Microsoft, as part of our drive to create a more trustworthy computing environment, we are significantly stepping up our efforts to fight spam and its pollution of the email ecosystem. Although there is no easy fix, we believe that spam can and must be dramatically reduced. We're working toward this goal on many fronts, through technological innovation and in partnership with other leaders in industry and government.
In this mail, which you're receiving as a subscriber to executive emails from Microsoft, I'd like to offer some insights into the work we are doing to counter spam.

Creating New Anti-Spam Technologies and Strategies

Because spam affects consumer and business users of many Microsoft products and services, we have been working for several years on spam filters, and on tools that enable people to block unwelcome senders and designate others as safe. These tools have become available in recent versions of products such as MSN, Hotmail, Exchange and Outlook.

Recognizing the increasing urgency of the issue, we recently created a new Anti-Spam Technology and Strategy Group that brings together specialists from across the company and integrates all of our anti-spam strategy and R&D efforts. We are building on advanced work at Microsoft Research in fields such as machine learning - the design of systems that learn from data and grow smarter over time. This kind of technology is vital to the fight against spam because every defensive action causes spammers to change their attack. Technology, to be effective, must continuously adapt, without requiring a team of people to examine messages one by one. With machine learning, a "smart" spam filter can automatically adjust to spammers' shifting tactics. A smart filter can also be customized to suit the preferences of an individual user. This is important because, although a lot of spam is pure junk, not all of it is clearly distinguishable based solely on broad, global criteria. Deciding precisely where to draw the line must ultimately be up to the individual. However, a smart filter can learn from a user's personal preferences to create a unique, anti-spam immune system that is much harder for spammers to work around.
Already, filters on the servers at MSN and Hotmail block more than 2.4 billion messages a day, before they ever reach our customers' inboxes. And to help deal with mail that survives this first hurdle, MSN 8 software includes a smart filter that becomes more effective over time as it learns the characteristics of mail that an individual customer regards as spam. This month, we updated MSN 8 with further improvements in its spam technologies, giving customers an option to block offensive images in email, and adding the ability to filter mail in languages besides English. We will offer more technology advances in a new release of MSN software later this year.

Meanwhile, we are working to create new anti-spam technologies that are even more precise, easier to use, and adaptable. And we are working to integrate them into more of our products, particularly Outlook and Exchange.

To help, we have assembled a massive and still growing database of spam, collected from volunteers among our millions of MSN and Hotmail subscribers. This database will prove invaluable later this year when we release Outlook 2003, which will include a new, smart filter that will access the database to recognize and block spam more effectively. The filter in Outlook 2003 also will be updated frequently and easily, as with Windows Update today.
Exchange 2003 includes a host of anti-spam features, including an Application Programming Interface that enables third-party providers of spam filters to easily supply solutions for Exchange customers. We plan to add our own smart filter and continue building more anti-spam capabilities into the Exchange messaging infrastructure. Our goal is to do everything we can to secure email systems with servers that monitor and control the points of entry. As we develop new technologies, stemming the tide of spam also requires a multi-faceted approach that includes industry self-regulation, effective and appropriate legislation, and targeted enforcement against the most egregious spammers. It also calls for cooperation among the major players in the email ecosystem. In April, we joined with AOL and Yahoo! in announcing a wide-ranging set of initiatives to fight spam together. Since then, Earthlink and others have joined the effort, which involves promoting business guidelines, best practices and technical standards that can help curb spam sent or received via any online service or computing platform.

Stopping Spam At the Source

Every major provider of email services has rules against spamming. Microsoft puts significant resources into investigating consumer complaints about spam that may have originated from accounts on MSN or Hotmail. We are firm in shutting down those who violate our anti-spam account policies.

There are other challenges. For example, spammers set up many different email accounts to avoid detection, and, once detected, they move to other services. To put an end to this shell game, we are taking steps to prevent spammers from creating fraudulent email accounts in bulk. We also are working with other service providers to share information so that we can keep tabs on roving spammers and shut them down more effectively.
Government policymakers also have a role to play. We support U.S. federal legislation that would strengthen the ability of service providers to shut down spammers by suing them on behalf of customers. And we believe that the use of automated searches to harvest addresses published on the Web and in Internet newsgroups should be banned, making it much more costly and difficult for spammers to assemble mailing lists.

Bringing Spammers into the Sunshine

Government and industry working together also can put an end to spammers' deceptive practices. Spammers go to great lengths to conceal or "spoof" their identities. They relay their mail through multiple servers to hide its origins. They open multiple accounts and change to new ones frequently to avoid drawing the attention of service providers, and to improve the chances of their mail passing through spam filters. They lure unsuspecting readers by faking sender addresses - ones that appear to be someone inside the recipient's company, for example.

Microsoft is working with others in the industry to identify and restrict mail that conceals its source. For example, we are working toward a system to verify sender addresses, much as recipients' addresses are verified today. The Internet addresses for all incoming mail servers are published as part of the Domain Name System, the Internet's distributed directory. That's how mail gets to the right destination. If domain administrators could also publish the addresses of their outgoing mail servers, then the receipt of a suspected forgery could trigger a relatively simple, automated verification process. Incoming servers would then be able to confirm whether senders are who they say they are.
To help fight fraudulent or otherwise illegal spam, we are cooperating with other service providers to create better mechanisms for preserving electronic evidence of spammers' activities. And we are coordinating civil lawsuits and other enforcement actions for greatest impact. On June 16, Microsoft filed 15 lawsuits in the United States and the United Kingdom against companies and individuals alleged to be responsible for billions of spam messages sent in violation of state and federal laws.

These efforts would be helped - and consumers would benefit - from legislation that would include clearer prohibitions against using misleading sender addresses and other false header information.

Isolating Spam

Part of the challenge in curbing spam lies in accurately identifying legitimate commercial email. What would help are guidelines defining, for example, whether and when an email is legitimate based on a previous business relationship between the sender and recipient. By drawing a clear line between spam and legitimate mail, guidelines would enable spam filters to work more precisely, and make it easier for honest businesses to stay on the right side of the line. Developing such guidelines is the focus of talks involving Microsoft and other technology leaders, responsible marketers and consumer groups. We favor the idea of setting up independent email trust authorities to establish and maintain commercial email guidelines, certify senders who follow the guidelines, and resolve customer disputes. Similar authorities already help in protecting people's privacy online, with organizations such as TRUSTe and BBBOnline providing certification for Web sites and companies that follow guidelines on the use of customers' data.

Self-regulation needs to be supported by strong federal legislation that empowers consumers without threatening the vitality of legitimate e-commerce. Our proposal is to create a regulatory "safe harbor" status for senders who comply with guidelines. The guidelines would be subject to approval by the Federal Trade Commission. Compliance would be confirmed by a self-regulatory body. Senders who do not comply would have to insert an "ADV:" label, for advertisement, in the subject line of all unsolicited commercial e-mail.

Computer users could then customize their spam filters to either accept "ADV:"-labeled mail or automatically delete it. Enabling consumers to regain control of their inboxes in this way would dramatically reduce the volume of spam by creating strong incentives for businesses to make sure their communications are consistent with best-practices guidelines developed by industry itself.

Changing the Landscape, Soon

These and other efforts across many fronts should lead to a world where we are less troubled by spam. As less of it reaches recipients - and violators face stiffer sanctions for illegal activities - the financial incentives for spammers will decrease, and spamming will lose much of its appeal.

At Microsoft, we're strongly committed to the goal of ending today's spam epidemic. If you'd like more information about our work on spam, and about steps you can take today to help protect yourself, it can be found here.

Bill Gates

****

Information Sharing under the Crime & Disorder Act 1998.

The 4 relevant authorities specified in the Act have changed over time. Health in particular is vested in PCTs now rather than Health Authorities. Those protocols you drew up nearly 5 years ago are in need of review. Other bodies can now enter into such data sharing arrangements. Who's in? Fire Authorities, Health and Registered Social Landlords. How do I find out how – Look at the Police Reform Act 2002. The relevant sections of the act are 61 and 97 but you'll see more plain English in the Explanatory notes section 335 and 470.

Click on http://www.legislation.hmso.gov.uk/acts/acts2002/20020030.htm and for the explanatory notes click on http://www.legislation.hmso.gov.uk/acts/en/2002en30.htm

****

Lord Chancellor's Dept Final Flourish

Before they disappeared the department started putting out some very useful material. Click first on http://www.lcd.gov.uk/foi/dpasaguide.htm for a very handy guide on subject access.

****

New Irish Data Protection Legislation

Ireland's new Data Protection (Amendment) Act 2003 means that it has finally implemented the 1995 EU Directive on Data Protection, almost five years after the expiry of the deadline. The Act amends rather than replaces the country's 1988 Act. France has still to comply.

****

New Privacy Law – The Zeta Jones Decision

In April, Michael Douglas and Catherine Zeta-Jones won a High Court ruling that said Hello! magazine breached their rights of commercial confidence by publishing photographs of their wedding. The couple sold the exclusive photo rights to the event to OK! magazine for £1 million,. A paparazzo intruder gained access to the wedding by bribing staff and surreptitiously took photographs, which were then bought by Hello! It then published the unauthorised photographs on the same day as OK!s authorised coverage.
Mr Justice Lindesy ruled that there was no existing law of privacy under which the Douglas's were entitled to relief. The introduction of such a law was better left to Parliament. However they were entitled to damages for breach of commercial confidentiality as being celebrities they were would normally expect to control their image and receive substantial payment for rights to their photos on such an occasion.

With regard to the Data Protection Act 1998, it was ruled that Hello! could be taken to be Data Controllers, the unauthorised pictures represented personal data, and publication of them was processing covered by the Act. The publication was held as not fair under the First Data Protection Principle. However this did not add a separate route to recovery for damage or distress beyond a nominal award.

The full judgement can be read on the Court service Website at www.courtservice.gov.uk

****

Irish Freedom of Information Act Request

An Irish internet campaigner has used the country's Freedom of Information Act to force University College, Dublin (UCD), to disclose documents that detail its operation, under accusations of mismanagement, overpricing and inefficiency.

Antóin Ó'Lachtnáin, has long complained that the .ie registry, run by UCD, is run in "a very untransparent fashion." Despite objections from UCD, he has now received written confirmation from Ireland's Information Commissioner that he is entitled to see the files and has posted a copy of the letter on his website. The college has 8 weeks to comply with the information request.

This case shows the impact of freedom of information on public bodies. Similar requests can be expected once the FOI Act comes fully into force in England and Wales in January 2005.

****

Schools and FOI

The FOI Act also applies to schools colleges and universities. They have until 31st December 2003 to submit their publication schemes to the Information Commissioner fro approval. The schemes, once approved, will go live at the end of February 2004.
Have you raised awareness amongst your education sector? Do schools and colleges know what to do? Have they started writing their publication schemes? Help is at hand. We are running another freedom of information workshop in Manchester on 5th November. See www actnowtraining.co.uk for details.

****

New Employee Monitoring Code

The Office of the Information Commissioner has now produced part 3 of the Employment Practices Data Protection Code that relates to monitoring and surveillance at work. The Commissioner has said :
"The fundamental message is that, where monitoring does take place, employees should be made aware of its nature and extent and the reasons for carrying it out. Only in exceptional circumstances will it be appropriate for employers to monitor their employees without their knowledge."

The Code is not legally binding but will be taken into account by the Commissioner and the Courts when considering any potential breaches of the Act. It is therefore essential that all organisations read and implement the code ASAP. The Code recommends that before doing any monitoring/surveillance of employees it is best to carry out by an "impact assessment". Such an assessment must consider the following points:

The purposes behind the monitoring;
Any likely adverse impact on the employee(s) or others – such as customers;
Alternatives to monitoring, or to the type of monitoring suggested;
The obligations that will arise; and
Whether the monitoring is justified.
In considering any likely adverse impact the employer must take into account:
The likely intrusion into employees' private lives
The extent to which the employee will be aware of the monitoring
Who will see the information, which may be sensitive
The impact on the employment relationship
The impact on other professionals – e.g. solicitors – who may have confidentiality issues

How the monitoring will be perceived – e.g. will it be seen as "oppressive" or "demeaning"?
The Code also makes good practice recommendations to ensure compliance with the 1998 Act.

In summary these are:

Managing data protection: identify the person with compliance responsibility, and set in place a mechanism to check that procedures are being carried out.
The general approach to monitoring: monitoring is intrusive and employees are entitled to keep their private lives private. Monitoring should take place for a clear, justified purpose, and employees should be aware that it is taking place.
Monitoring electronic communications: create a policy on the use of such communication tools and let employees know what it is. Make sure that the Regulation of Investigatory Powers Act, and the Lawful Business Practice Regulations, which govern interception of e-mails, telephone calls etc, are complied with.
Video and audio monitoring: let employees, and all others who may be caught on camera, or on tape, know when this is being carried out, and why.
Covert monitoring: should be authorised by senior management, and strictly targeted. Only to be used for suspected criminal activity, where notification would hinder the detection of the activity.
In-vehicle monitoring: develop a policy on private use for work vehicles, and let employees know about it.
Monitoring through information from third parties: let employees know what sort of checks are going to be made, and why
The full code and guidance notes can be read on the Commissioner's website www.dataprotection.gov.uk. Part 1 and 2 of the Code relate to the Recruitment and Employment Records respectively. Please see www.actnow.org.uk for articles on these. Part 4 of the Code on medical records is promised in the next few months by the OIC

****
Campaign For Freedom of Information Update

1) The Cabinet Office has finally accepted the Campaign's argument that the names of private sector staff seconded to government departments should normally be disclosed, even if the individuals concerned or their companies object. The test in the future should be whether disclosure would cause some specific harm to the individual, and even then the public interest in revealing the names must also be considered.

The Cabinet Office has revised its guidance to Whitehall on the matter. The decision follows a three year campaign, in which the Campaign has in turn successfully challenged the DTI, the Treasury, the Foreign Office and now the Cabinet Office to reverse their policies on the issue.

See: http://www.cfoi.org.uk/secondees.html

2) The Department of Health has indicated that it will amend its guidance on access to health records to comply with the two ministerial promises that the Campaign showed had been broken. This should lead to patients getting quicker access to their health records and being allowed to add their own views about a disputed matter to the record.

See http://www.cfoi.org.uk/dohltr100103.html .

3) The Campaign has produced an electronic version of the Government's Guidance on Interpretation of the open government code. This was not previously available on the Internet and has been reproduced with the permission of the Department for Constitutional Affairs (formerly the Lord Chancellor's Dept).

See: http://www.cfoi.org.uk/opengov.html#og

****

Video Surveillance Evidence - Jones v University of Warwick

This was a personal injury action (February 2003 Court of Appeal) in which the claimant alleged significant continuing disability in her right hand. An enquiry agent instructed by the defendant's insurers posed as a market researcher to gain access to the claimant's home and filmed her with a hidden video camera. The defendant contended that the film showed that contrary to the claimant's case, she had an entirely satisfactory function in her right hand.

The court held that in this case the conduct of the defendant's insurers was not so outrageous that the defence should be struck out which meant that it must be tried. To exclude the use of this evidence would be wholly undesirable. Fresh medical experts would have to be instructed and relevant evidence withheld from them, perhaps leading to a misdiagnosis. The claimant could not be cross-examined properly. However, the court could reflect its disapproval of the defendant's conduct in its costs order. In this case, subject to hearing further submissions, the court proposed to order the defendant to pay the costs of the initial hearing and two appeal hearings on this issue.

This case should be read in the light of the Regulation of Investigatory Powers Act which imposes obligations on, amongst others, local authorities when carrying out any kind of covert surveillance and monitoring. The Act is backed by an inspection carried out by the Office of the Surveillance Commissioners.

We are running a course on RIPA at the National Railway Museum in York on October 23rd. See www.actnowtraining.co.uk for full details. We have also run a number of in house training sessions on the Act for officers who have to work with it e.g. environmental health, planning, trading standards, benefit fraud investigators etc.

****

Mary Bell and the Right of Anonymity

X, a Woman formerly known as Mary Bell (2) Y v (1) S (2) News Group Newspapers Ltd (3) MGN Ltd (2003)

This case concerns Mary Bell and her daughter who sought lifetime anonymity to protect them from intrusion by the media and any disclosure of their identities, or details of their lives that might identify them.

The Court held that an injunction was justified on human rights grounds in particular the right to privacy and the right to life bearing in mind, amongst other things, Mary Bell's fragile mental state, her rehabilitation process and the serious risk of physical harm to herself and her daughter.

****

Police Naming and Shaming

R. (on the application of Ellis) v the Chief Constable of Essex Police

In the April newsletter we covered this case where the he Court was considering the lawfulness of an "offender naming scheme" operated by Essex police in light of an individual's right to respect for private and family life under Article 8 of the European Convention on Human Rights. At that stage the offender got an interim injunction preventing him being named and shamed in this way.

On June 12th 2003 the High Court considered the case further when the interim injunction granted in April expired.

The objective of the scheme was to reduce burglary and car crime in the Brentwood area, and it was implemented by Essex police in an attempt to carry out their duties under the Crime and Disorder Act 1998, under which they sought to implement strategies for reducing crime. The police believed that the posters would help deter youngsters from getting involved in crime, and would demonstrate to victims that the criminal justice system was effectively dealing with crime head-on.

The court concluded that as regards this point it would need to consider each and every case on its particular facts. Furthermore, the court stated that in all cases there should only be disclosure where there was a "pressing need" to make details available to the public by way of this or any other similar scheme, whilst the police should always consider the views of all other agencies as fully as possible.

Furthermore, the court made it clear that had it been necessary to rule on E's individual case it would have done so in E's favour on the grounds that Essex police had not given adequate consideration to the concerns of the probation service. The court also took into account the potential damage that could have been done to E's family and child despite their change of address, as they had rights under Article 8 that must also be considered. The court made it clear that similar factors would be considered in every case such as this, where an individual's fundamental freedoms were being challenged by the demand to publicise details of the individual and the offence that he/she may have committed.

In addition, the court raised a number of concerns that would certainly be pertinent to any future consideration of this type of case. In particular, the court felt that even if the scheme were to be considered in the future it would certainly be questionable as to whether the inclusion of the father or mother of a young child would ever be acceptable. A serious question mark was also raised over the fact that the inclusion of an individual in such a scheme could mean that that person was being unfairly discriminated against and this could be seen as a form of additional punishment.

Overall, the Court made it clear that it did have reservations in respect of the use of the scheme, principally for those reasons set out above, although in this case it would not be drawn into making a ruling as to whether the scheme was in principal lawful or not. Indeed, its legality depended on the particular circumstances of each offender included in it and how the scheme operated in practice.

Therefore, it remains to be seen whether the need to preserve an individual's rights under Article 8 can ever be outweighed by the potential benefits that could be delivered by a scheme such as this. The law in this area therefore remains to be tested fully and whilst one may speculate based on the decision of the court in this particular case, the legality of the scheme still remains unclear. Whilst the reasons given by the court in this case give a feeling that its principal concern was for the protection of the individual's rights, there is plenty to be said for the fact that in future cases a different set of circumstances surrounding the case and the individual in question could well produce a very different outcome.

****

If you are a commercial lawyer in local government the above site will interest you. It contains free resources, links and articles on data protection, freedom of information, IT Law, PFI, EU Law and many other aspects of commercial law. There is a free bulletin board to float your queries and ideas to over sixty other members from all over the UK. You can also take advantage of free/discounted courses. Click on http://groups.msn.com/LGGCommercialLaw It's free and you may find something of use.

****

Training in Information Management issues

Act Now offers a programme of high quality but low cost Training courses at city centre venues throughout the UK or can come to you and deliver training in-house. We can train 50 people at your premises for the price of 2 delegates at an expensive London course. Obtain best value for your organisation. Our speakers work in the public sector and bring up to date expertise to the training courses. Contact Act Now for details.

****

Act Now is a trading name of Act Now Training Ltd
Registered Office, Selbourne House, 26 Selbourne Avenue, Dewsbury, West Yorkshire, WF12 9PA
Fax 01924-520242, Email info@actnowtraining.co.uk

****

Disclaimer The contents of this web newsletter are meant for you to consider on the basis of general discussion and not as advice or expert opinion (legal or otherwise). The views expressed do not reflect those of our respective employers. You should obtain professional legal advice on any specific issues. Any liability (in negligence or otherwise) arising from you acting, or refraining from acting, on any information contained in this newsletter is excluded.

Copyright Copyright belongs to ActNow and we ask that anyone who wishes to subscribe or unsubscribe to our newsletter does so via our website form. Your information will be used only for the purposes of this newsletter and in accordance with the Data Protection Act 1998. Public Sector organisations can re-use material within their own organisation if they acknowledge our contribution by linking to our website.