IP addresses and personal data: K.U. v Finland

Karen McCullagh
2008: the year of data insecurity
Contents

3  Editorial

4  UK News

14  Foreign News

24  Analysis – Data Protection Compliance in Israel’s Pension Fund Industry Reform

28  Analysis – National Information Assurance Agenda

32  Data Protection Courses

34  Soapbox
The final quarter of 2008 rounded off a year in which data protection continued to be projected into the public eye. In his speech to RSA (the Security Division of EMC Corporation) Conference Europe in October the Information Commissioner labelled it the year of "data insecurity", a year which "has undoubtedly been the year of data breaches and data losses." From November 2007 up until the time of his speech the number of data breaches reported to his office had soared to 277. Our Soapbox feature in this edition focuses on the Commissioner’s speech.

Five documents relating to Government information were published in the aftermath of a number of well publicised security lapses in the public sector. Since those publications the losses of personal data through access to the “Government Gateway” website, personal data of the Ministry of Defence employees and its applicants and personal data of all prisoners in England and Wales, have all been revealed. The media scrutiny of the approach towards the management of information security by the public sector remains intense and we centre our attention, in one of the analysis pieces, on the Government’s National Information Assurance Strategy (NIAS). The NIAS has been the subject of an independent assessment by Nick Coleman, former head of IBM’s security services division. The findings reveal that there are still many gaps which need filling. The Government has also responded to the Data Sharing Review Report, by strengthening its powers to share data. Legislation will introduce a fast-track procedure to allow data sharing whenever “a robust case” can be made for sharing. There will also be a statutory duty on the Information Commissioner’s Office to prepare a code on the sharing of personal data, but as with the other codes which have been produced under the Data Protection Act (DPA), this is not a statutory code.

As reported in the last edition, the ICO has been given the ability to fine organisations if their operational procedures cause a gross breach of data protection principles. This new power is found in the new section 55A of the DPA (through section 144 of the Criminal Justice and Immigration Act 2008) but it is yet to be confirmed when the powers will come into force or what the maximum fines will be. The Government has also announced that the Information Commissioner will be able to perform spot-checks on government departments and public sector bodies to make sure they are complying with the DPA. Further, the funding arrangements of the ICO are set to change with a tiered fee structure based on size of organisation replacing the current flat-rate notification fee of £35. This has been considered before and has faltered at the administrative stage.

As we enter 2009 it remains to be seen whether proposed stronger enforcement powers and an increase in accountability will increase public confidence in the Government’s handling of data.
The Information Commissioner’s inspection powers and funding arrangements under the Data Protection Act 1998 (DPA)

On 16 July 2008 the Ministry of Justice (MoJ) opened a consultation on proposed changes to the Information Commissioner’s inspection powers and funding arrangements. The consultation closed on the 27th August and various interested parties have now responded to the proposals.

The recommendations in the consultation stemmed from the Data Sharing Review recently conducted by Richard Thomas, the Information Commissioner, and Dr Mark Walport, Director of the Wellcome Trust, an independent charity which funds research to improve human and animal health.

A key conclusion of the review was that in order to effectively carry out his duties, the Information Commissioner needs stronger and more versatile sanctions.

Specifically, the review proposed the following:
- Introduction of measures to allow data controllers to provide a Good Practice Assessment (GPA) when they register with the Information Commissioners Office (ICO);
- Introduction of an exemption from section 55A of the DPA (financial penalties applicable where there is a breach of the DPA) discovered in the process of a GPA where a data controller has provided to consent to such GPA;
- Introduction of a 3 month notice period for data controllers to withdraw from a GPA (to prevent a data controller from agreeing to a GPA on registration only to immediately withdraw once registration is completed);
- Enhancement of section 43 DPA to enable the Commissioner to specify a time and place that any information should be provided under an Information Notice;
- Strengthening of the ICO powers under Schedule 9 of the DPA to enable the Commissioner to demand information during an inspection to determine whether a data controller is complying with the principles of the DPA;
- Consideration of an amendment to Schedule 9 of the DPA to allow the Information Commissioner to apply for a warrant in cases where he does not have reasonable grounds to suspect breach of the principles of the DPA;
- Introduction of a tiered notification fee structure to recognise different sized organisations; and
- Introduction of a new sanction for data controllers who knowingly or recklessly provide incorrect information as part of their notification fee self assessment.

Questions from the consultation have led to a mixed response from interested parties. The main issues have centred on the structured approach to GPA and the blanket indemnity from monetary sanction and the proposal to extend Schedule 9 of the DPA to allow the Information Commissioner a warrant in cases where he does not have reasonable grounds to suspect a breach of the principles of the DPA.

The Information Commissioner himself has questioned the proposed amendments to GPAs, as this would appear to be at odds with his aim to streamline the notification process for data controllers.
Other organisations such as Justice and the British Computer Society have suggested that rather than taking a punitive approach to non-compliance under a GPA, the GPA is used as a cooperative process and a tool for raising compliance standards. The BCA suggests it should be considered as a Kite Mark for compliance.

The strongest criticism though is reserved for the proposed amendment to Schedule 9 with most respondents suggesting that the ability to obtain a warrant to inspect business premises, without reasonable grounds to suspect non-compliance with the DPA, would be unacceptable.

The consultation has now closed and the next step for the MoJ will be to collate and summarise all the responses. Once done consideration can then be given to the implementation of the suggested powers. What can be said with certainty is that the DPA enforcement landscape will be in for significant changes over the coming months.

Watch this space.

Recent security breaches

This article will look at a number of high profile security breaches that have occurred over the past few months.

Home office and PA Consulting

In August PA Consulting, a contractor working for the Home Office, had its contract terminated after admitting to the loss of a memory stick which held the personal data of all prisoners in England and Wales. The information was not encrypted.

The information, sensitive personal data under the DPA, consisted of the names and dates of birth of all of the 84,000 prisoners in England and Wales as well as the names, addresses and dates of birth of 33,000 prisoners in rehabilitation. The information was held on the contractor’s site and was downloaded for “processing purposes” on to the memory stick. The stick was left in an unlocked drawer in an unsecured office.

The Home Secretary stated that the information had been transferred securely to PA Consulting and that appropriate security provisions had been agreed with PA Consulting but that these had not been followed by the contractor. PA Consulting claimed that it had robust information security provisions in place but that these had not been followed by a particular member of staff. Other contracts between the Government and PA Consulting (including their role in the ID cards scheme) are under review.

Ministry of Defence

In October, the Ministry of Defence (MoD) admitted the loss by one of its contractors, EDS, of a computer hard drive which may have contained the personal data of up to 100,000 armed forces personnel and 600,000 applicants.

Neither EDS nor the MoD were able to confirm whether personal data was held on the hard drive or exactly when the hard drive went missing. The information may though have included names, addresses, dates of birth and bank details. The hard drive was not encrypted. The loss was revealed following an audit required by the Cabinet Office.

In a statement, EDS said that although there was "no evidence that security at [the EDS] site had been breached" it "was unable to account for a removable hard drive". The hard drive was part of a test involving "TAFMIS", the Armed Forces training and financial management system and was stored at EDS’ facility near Basingstoke.

The MoD was the subject of Sir Edmund Burton’s investigation in January 2008 following the loss of laptops owned by the Navy containing personal data of applicants. The report found that there were “departmental failings” in terms of the MoD’s oversight of personal data relating to Armed Forces personnel and that there was a “very limited understanding of the Department’s obligations under the [DPA]”. The MoD accepted the report’s conclusions and had agreed to implement the recommendations for tighter security.

Government Gateway

In November, a computer memory stick containing usernames and passwords for accessing the “Government Gateway” website was found in a pub car park.

The website allows people to register for the use of a number of public services, including tax and benefit claims. The memory stick was the property of Atos Origin, a contractor responsible for the running of the website. Atos Origin issued a statement that one of their employees had “misplaced” the stick and had breached company procedure in removing the device from the company’s premises.
The Department for Work and Pensions denied that the information would allow access to the personal data of 12 million individuals which is stored on the site, stating that the passwords were for an earlier version of the site. An "urgent investigation" is under way.

Deloitte

In October, a laptop belonging to a Deloitte & Touche employee was stolen from a handbag in a public place. The laptop contained information relating to the pensions of 150,000 railway workers as well as all UK Vodafone staff with pensions (including names, NI numbers and dates of birth) and other unspecified information.

Deloitte has stated that the information on the laptop was encrypted and that the laptop was password protected. Deloitte further stated that "[it] has information security policies which include guidelines for employees to ensure they pay close attention to their laptops when in public places. Nevertheless, and very unfortunately, this theft still occurred."

Commentary

As we go to press, the ICO has just published Privacy by Design, a guidance note about the need to be proactive in data protection matters. It is advisable to review the reliability of contractors and the robustness of any contracts in place, and to reinforce the need for training of data protection issues to staff.

The National Consumer Council asks EU for security breach law

The National Consumer Council (NCC) has called on the European Commission to force companies who lose customer data to admit the error publicly. The NCC believes a data breach notification law is a necessary incentive to force companies to keep data more securely.

This request has been prompted by the European Commission’s recent publication of a package of reform measures for the telecoms industry. The package contains a proposal that internet service providers should be forced to disclose any data breaches. The NCC has called for the proposals to be extended to banks and other businesses collecting significant amounts of personal data. It argues that forcing companies to notify breaches will act as an incentive for them to treat data more carefully due to the threat of reputational damage.

However, a number of parties have voiced concerns, including the Information Commissioner’s Office, and have said that they do not want such a law to be introduced in the UK. The usefulness of such laws are challenged on the basis that notification of too many data breaches may “desensitise” the public to the effect of the really serious breaches of security and further, there is a risk that the regulators will become inundated with notifications making it difficult to evaluate the really serious breaches.

There is an argument that notifications of data breaches will become all too common and people will become tired of receiving them. By the same token, people’s heightened awareness of the security breaches may make them more skeptical about handing over their personal data which may result in them generally loosing faith in all organisations that handle data. Ultimately, this will not serve to tackle the security breaches and will only worry consumers.

The Information Commissioner argues that the key to the success of such laws would be to ensure that the threshold of their application is applied correctly i.e. that only the serious breaches are notified. A balance needs to be struck between the level of risk to the data subjects, the harm which might result, the type and quantity of data lost and an appropriate penalty to incentivise data controllers to ensure the adequate security of the data. There is a need to focus on the detriment of the data breach on the individual, the organisation itself and society as a whole. The Information Commissioner is best equipped to perform such an evaluation and therefore reporting incidents of data security breaches to the Information Commissioner remains perhaps the best course of action.

More recently the Ministry of Justice has publicly announced that it agrees with the Information Commissioner and that as a matter of good practice, security breaches should be notified to the Information Commissioner to ensure...
that appropriate remedial action is taken. The Information Commissioner has published guidance for data controllers on when breaches of security should be notified. The Ministry of Justice has stated that failure to do so will be taken into account by the Information Commissioner in any enforcement action.

In addition the NCC has called for the increase of powers of the Information Commissioner in particular to deal with negligent breaches of security. Only recently the Criminal Justice and Immigration Act 2008 introduced the power of the Information Commissioner to impose monetary penalties for a serious contravention of the DPA’s principles. This power is not yet in force and we are yet to experience its impact, in particular how it will be used by the Information Commissioner and the level of fines imposed.

However, according to the Information Commissioner’s Office in the past year they have received in the region of 277 notifications of data breaches across a variety of different sectors and industries (this is not to mention the more high profile data losses of the Government). Enforcement action has already been taken against the HMRC, the Ministry of Defense and the Department of Health by the Commissioner and it is likely that the Commissioner will take a more stern approach to such losses in the future.

Extension of the Data Retention Regulations

The Government has published the draft Data Retention (EC Directive) Regulations 2007 which will transpose the final part of the EC Directive on data retention. The new Regulations, set to come into effect on 15 March 2009, will extend the provisions introduced in 2006 requiring the retention of data relating to fixed and mobile telephony. The 2007 Regulations will also apply to data relating to internet access, internet telephony and e-mail.

The aim of the Directive is to ensure that data relating to electronic communications is retained to enable public authorities to investigate, detect and prosecute crime. Use of electronic communications data has become increasingly important to law enforcement agencies in performing their duties effectively. The need for regulations surrounding the retention of data was cemented by the 7/7 bombings that took place on the London transport network in 2007.

The new Regulations provide that all location data and traffic data generated by publicly available electronic communications services and networks must be kept for 12 months. This period may be reduced to a minimum of 6 months with the prior written consent of the Home Office.

“Location data” refers to any data processed by a network which indicates the geographic location of the user. “Traffic data” means any data processed when sending a communication on a network or for billing the user. The Regulations set out the data to be retained, which includes data to identify the source, destination, date, time, length and type of communication.

The meaning of “providers of publicly available electronic communications services” and “public communications networks” is open to interpretation by each EC member state.

In France and Italy, it is expected that it will apply to internet cafes, bars, restaurants, hotels, and airports, to the extent that they provide services such as public internet terminals. On the other hand, preliminary discussions in Germany and Spain suggest that they are likely to adopt a narrower interpretation which will include only entities that directly provide telecommunication and internet access services. It remains to be seen which approach the UK will take. These new Regulations will have a severe impact on public service providers and public network providers, particularly those who do not currently retain the data they capture.

There is no need to generate the information specified, only to retain information which is captured. Critically, the Regulations will not apply to a public communications provider if the data is being retained by another communications provider. This provision should have a significant impact due to the number of public communications providers in the industry who provide their services using another public communication provider’s network.

The potential cost of compliance has been acknowledged by the Government. The new Regulations, together with the Anti-terrorism, Crime and Security Act 2001, provide that the Government may give a grant to public communications service or network providers to cover these costs. Any such request needs to be notified and agreed in advance.

Recent information shows that the average grant size has risen from £17,000 in 2004 to £830,000 in 2007 suggesting that many are taking advantage of this funding.
Disclosure of employee information under TUPE

The Information Commissioner’s Office published new guidance to help organisations comply with the Data Protection Act when providing information about their employees under The Transfer of Undertakings (Protection of Employment) Regulations 2006 (TUPE).

TUPE is designed to preserve the employee’s terms and conditions when a business or undertaking is transferred to a new employer (including where there is a service transfer, for example an outsourcing).

When a business, undertaking or service is transferred, TUPE requires the employer to provide details of the employees transferring to the new employer before the transfer takes place. Whilst the transfer of data under TUPE is a legal requirement, this creates obvious issues under the Data Protection Act 1998 (DPA). The issue that arises is how can TUPE and the DPA work together so that the employer can comply with both Acts?

TUPE requires the following details to be given to the new employer before the transfer takes place:

- identity of the employee;
- information from the employee statement of particulars including their hours of work, holidays etc;
- information on any collective agreements;
- details of disciplinary actions or grievances in last two years;
- information about any legal action taken by an employee against the employer in the last two years or details of any potential actions.

Section 35 of the DPA allows for disclosure of this information, as it is required by law under TUPE. In fact employers will face penalties if they do not disclose the information but the disclosure must still comply with the other principles of the DPA.

In particular, information must be accurate, up to date, kept secure and should only be used for the purposes of assessing matters associated with the transfer of the employers to the new employer. The personal data transferred to the new employer should be limited so that irrelevant or excessive personal data should not be sent.

Employers need to remember that the DPA should be considered early on in the discussions regarding the transfer to the new employer. The Information Commissioner suggests that as far as possible the information to be transferred and the method of transfer should be agreed beforehand so that the security of the personal data can be protected. If requests for information by the new employer go beyond the required disclosures under TUPE then the employer should consider to what extent the information can be anonymised and it is recommended that the employer should, where possible, obtain consent.

After the transfer of the employees has taken place the former employer should consider its obligations in relation to retention of data, any information that the former employer does not need to keep should be deleted or destroyed (remember that information should not be kept on the basis that it may become useful in the future). The new employer, once the transfer is complete, will require further information in order to manage the workforce and run the business. However, the new employer should check that the personnel files do not contain any information which is not required and should then be deleted or destroyed.

The Information Commissioner’s guidance is a good starting point to consider before any transfer but the key message here is that whilst the disclosure of employee data is a legal obligation under TUPE don’t forget the Data Protection Act 1998!
APNR – The largest database in Europe?

The Guardian newspaper recently obtained Home Office correspondence revealing that data on millions of innocent motorists captured by the Automatic Number Plate Recognition (APNR) cameras is being held for up to 5 years. This is an “unnecessary and disproportionate” period of time according to Privacy International, a human rights group, in their official complaint to the Information Commissioner’s Office (ICO). The ICO has responded by saying that it takes the complaint seriously and will be approaching the police to discuss proposed data retention periods.

The APNR system, launched in 2005 with over £30 million of investment, was piloted for six months by nine police forces. Following the success of that pilot, it has since been rolled out to half of all police forces in England and Wales and, by the end of this year, it is expected to be run by all but two forces. By 2009, the APNR system will be recording up to 50 million licence plates a day and will be able to store as many as 18 billion sightings – making it possibly the largest database in Europe.

The purpose of collecting the data is to assist the police in the detection and prevention of crime. The Association of Chief Police Officers claims that there are very strong links between illegal use of motor vehicles on the road and other types of serious crime and that awareness of the database will deter criminals because of the increased chance of detection. During the 2005 trial, the ANPR database assisted the police in seizing more than £100,000 in illegal drugs, recovering over 300 stolen vehicles (worth more than £2 million) and stolen goods to the value of £715,000. More than 3,000 people were arrested – ten times more than the national average – with most of the arrests being for serious crimes.

However Privacy International’s issue is not with the purpose for which the data is collected but rather the length of time it is held for, particularly since the great majority of data subjects are innocent motorists. The fifth data protection principle of the Data Protection Act 1998 requires that personal data processed for any purpose should not be kept longer than is necessary for that purpose. Senior police officers originally claimed that the data would only be stored for two years but the Home Office recently admitted that the data is now being held for up to five years.

The ICO has advised that “prolonged retention would need to be clearly justified based on continuing value, not on the mere chance it may come in useful”. There is also a potential breach of the third data protection principle as retaining personal data that is not needed – i.e. data relating to highway users who are not criminals – could be deemed “excessive”.

The Information Commissioner has already raised concerns over the creation of the APNR database. Earlier this year in a statement to the press, he said that he did not believe there had been sufficient parliamentary or public debate on the centralised collection and retention of data from APNR cameras. With this latest complaint from Privacy International, now may be the time to make his actions speak louder than his words – otherwise, what has been touted as possibly the largest database in Europe may well be known as the largest illegal database in Europe.
The European Commission push for answers on BT’s trials of Phorm

The European Commission is analysing the Government’s explanation of why UK authorities failed to act over BT and Phorm’s allegedly illegal broadband wiretapping and ad-targeting experiments in Autumn 2006 and Summer 2007. The European Commission began investigating when the UK watchdog, the Information Commissioner’s Office (ICO), failed to punish BT and Phorm despite acknowledging that the trials had breached UK and EU data protection law.

Phorm Webwise is a controversial user profiling program which picks up addresses and content of certain websites visited by the user by piggybacking on the ISP network. The software then matches the profile with appropriate advertising allowing it to serve the user with targeted marketing. Despite assurances from the creators that the identity of the user cannot be discovered through this process, many critics believe that the user will be traceable from the data stream and thereby breaches data protection law. BT trialled the use of Phorm on consumer broadband subscribers.

The European Privacy and Electronic Communications Directive (the European Directive) requires that web users consent to particular uses of their traffic data and are given certain information as to the use of cookies. Phorm and BT have said that the technology does not breach Privacy and Electronic Communications Regulations (PECR), the UK law derived from the European Directive, in either of these respects, as customers are required to give informed consent before the software is used. However, during the trials in 2006 and 2007, customers were not invited to take part and were not informed the trials were going on. According to some reports BT denied any connection to Phorm and claimed that the unauthorised connections were a result of malware on users’ computers.

The ICO, which is responsible for enforcing PECR, previously confirmed that it would take no action over the tests. The ICO wrote to BT and agreed that:

“Whilst it does appear likely that a technical breach of the Privacy and Electronic Communications Regulations occurred in the 2006 and 2007 trials, there is no evidence to suggest significant detriment to the individuals involved. We acknowledge the difficulties that you have highlighted in providing meaningful information to customers about small scale, technical trials in circumstances like this.”

The European Commission has asked the UK’s Department for Business, Enterprise and Regulatory Reform (BERR) for an explanation of how the privacy of UK citizens was protected during the BT trials. This is the second time the European Commission has asked for clarification after the first response from BERR failed to address the legal issues surrounding BT’s secret tests.

There is still a possibility however that one of the web users affected could sue Phorm and BT for the breach of PECR. It is also unlikely that the European Commission will be as lenient in their assessment of the breach.

The news that Europe is not going to drop the issue adds further to Phorm’s woes. The Crown Prosecution Service has just announced that it plans to examine whether the BT trials of Phorm broke wiretapping laws. Further, Orange, the UK’s sixth largest broadband provider, has withdrawn from discussions to adopt the software on its network, explaining that the privacy issue was “too strong”.
ICO finds Liberal Democrats in breach of PECR

The Information Commissioner has found that the Liberal Democrats broke anti-spam laws by using an automated calling system to call 250,000 homes without consent. The calls, featuring a recorded message from party leader Nick Clegg, were made to households across the UK.

The Privacy and Electronic Communications Regulations (PECR) provide that prior consent is needed to use automated calling to promote a product or service. In this case, the Information Commissioner took the view that the purpose of the calls was to promote the Liberal Democrats and therefore constituted direct marketing. He ruled that the party should not have called anyone without their prior consent and rejected claims by senior party members that the calls were for "genuine market research", not promotion.

This view is entirely consistent with an earlier decision in 2006 against the Scottish National Party by the Information Tribunal, which made clear that the anti-spam laws cover political parties when they canvass support by telephone. It is also consistent with the views expressed by the Information Commissioner's Office (ICO) since rules on unsolicited marketing were first introduced in 1998. The ICO has consistently made clear that promotion of a political party is marketing and has contacted political parties to advise them of this on several occasions.

The Liberal Democrats were ordered to stop making the calls within 30 days of the Enforcement Notice issued by the ICO. Breach of an Enforcement Notice is a criminal offence and failure to comply with such a notice may lead to prosecution.

The speed in which the enforcement notice was issued is indicative of the eagerness of the ICO to take decisive action on breaches of the Data Protection Act and PECR. This is perhaps not surprising given the new powers to issue stop now notices and fixed penalties under the Regulatory Enforcement and Sanctions Act 2008 and the enhanced power to fine under the Criminal Justice and Immigration Act 2008 (although this is not yet in force). The level of fines which may be issued by the Information Commissioner is not yet clear, however the Information Commissioner made a case for fines of up to 10% of turnover in the Walport Thomas report. The ability to impose what would be significant fines, coupled with the Information Commissioner's desire to take decisive action on breaches, will act as a major deterrent to falling foul of the Data Protection Act and PECR in the future.

Communications surveillance plans on hold

The Government's plan to build a giant communications database has been postponed until 2009. The Home Secretary Jacqui Smith made the announcement in October but did not confirm whether the issue would be dropped from the Queen's speech which sets out the legislative programme for the year ahead.

The Government has encountered opposition from the ICO and a large number of politicians over the controversial plans, some of whom have gone as far as branding the concept "Orwellian". The weight of the issues raised has seen the Government agree to hold a public consultation so that people's concerns can be heard.

The plans would allow the Government to compulsorily acquire data held by phone companies and internet service providers and use it to create a central Government database. The database will store details of the fact (but not the content) of every e-mail, web session and phone call made in the UK, including its location, length and the identity of the caller or computer.

The Government already has the ability to log e-mail and phone communications. The new plans would see these powers extended to communications made via websites and internet-based phone technology, in an effort to capture the new generation of communications made on social networking sites.

In May 2008 the ICO released a cautionary statement in relation to the Government's plans:

"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", said Jonathan Bamford, Assistant Information Commissioner. He went on to say that "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."

The rationale behind increasing monitoring powers is to improve the effectiveness of law enforcement agencies. The ability to intercept communications and obtain communications data is central to combating serious crime and terrorism but the changing landscape of telecoms makes this increasingly difficult.

Speaking on Question Time, Transport Secretary Geoff Hoon strongly defended the proposals claiming that, "If [terrorists] are going to use the internet to communicate with each other and we don't have the power to deal with that, then you are giving a licence to terrorists to kill people". However, even Lord Carlile, the Government's own independent reviewer of anti-terrorism legislation has said of the proposals "as a raw idea it is awful". He warned that "very strict controls" would have to be introduced to limit the circumstances in which searches could be conducted.

It is likely that the consultation process will be protracted in an effort to fully explore the anticipated advantages and security doubts. Meanwhile the ICO has advised that it will be "studying the Government's proposals once published and responding to the Government's consultation in due course."
Almost every adult living in the UK today will have their credit records stored with one of the country’s three main Credit Reference Agencies (CRAs) – Experian Ltd, Equifax plc and Callcredit plc. Credit records are gathered from previous lenders and public records (such as the electoral roll and court records) whether the lending is by way of credit card, store card, mortgage or loan. Information is included about payments that have been missed. These records are currently available to financial institutions to carry out checks on whether that person is a good credit risk or not before offering credit. Most lenders will not lend without carrying out these checks although most will also ask for additional information in order to build up their own picture of the credit risk.

The new proposals would mean that credit records could be closed or “frozen” by the person to whom they relate and that institutions would need to ask for them to be unfrozen before they could be checked. In this way, Nick Clegg suggested that fraudsters would find it harder to obtain credit against someone else’s identity because the records could not be unfrozen without intervention by their true owner. Without the lender being able to carry out the checks, the fraudulent applications would be denied.

When outlining the proposals in October 2008 Nick Clegg said that they would provide a less intrusive, less expensive alternative to the Government’s ID cards proposal. He did not comment on who would be responsible for administering the freezing process and how long the freezing and unfreezing processes would take.

Most States in the US have had credit-record freezing laws in place for 2-3 years now, but the impact they have had on financial and ID crime has been questioned. Permitting records to be frozen does not prevent identity theft or funds being stolen, through online banking frauds or purchases made with cloned credit or debit cards. Consumers have also found the delay in unfreezing records can be very inconvenient when applying for legitimate credit – often it can take a few days for records to be unfrozen.

In the UK the Fraud Prevention Service, CIFAS, has reported falling levels of identity theft over the past 3 years. In fact in the past year the area of financial fraud that has reportedly shown the sharpest rise has been facility takeover fraud (where the fraudster hijacks an individual’s accounts in order to take control of them). The freezing measures proposed by the Liberal Democrat Leader would not help to prevent facility takeover fraud because it occurs after the accounts have already been opened. Quite what impact the proposed measures might actually have on financial and ID crime in the UK is therefore uncertain.

The issue of permitting checks to be carried out also raises concerns similar to those related to the giving of consent to data processing under the Data Protection Act. Organisations in the financial services industry in the UK carry out credit record checks as part of their pre-employment vetting procedures and may often repeat these checks on a regular basis throughout the course of the employment. This will therefore raise issues of how employees could consent to unfreezing their credit records to allow the repeat checks to be carried out.

It is clear that the proposed measures will require considerably more thought before they could be rolled out, and the experiences of the US will provide a useful background against which to do this, but it remains to be seen whether they are the best way of combating identity theft and the problems this causes.
Virgin Media found in breach of DPA

Reports of “missing discs” have hit newspaper headlines all too frequently over the past twelve months. Nationwide Building Society, Vodafone, Royal Bank of Scotland and the Home Office are some of the public and private sector organisations whose loss of data has resulted in high profile investigations. As companies begin to appreciate the legal and commercial ramifications of such data breaches, the recent decision of the Information Commissioner’s Office (ICO) in the Virgin Media case confirms the severe scrutiny which companies’ data processing procedures will face in the event of data breach.

Names, addresses and bank details of more than three thousand Virgin Media customers went missing in May 2008 when an unencrypted disc was lost in a transfer of data to Virgin Media from Carphone Warehouse. Virgin Media alerted the ICO at the time of the loss and informed all affected customers. In addition, it offered credit file protection to each customer.

Following an investigation by the ICO into the loss of the customers’ personal data, Virgin Media was found in breach of the DPA. The ICO has required Virgin Media to sign a formal undertaking, under which Virgin Media agrees to comply with the seventh principle of the DPA. The company has also been ordered to implement a number of security measures to ensure the effective protection of customers’ personal data. This includes encrypting all portable and mobile devices which transmit or store personal information and requiring any company which processes personal data on Virgin Media’s behalf to be explicitly required to use such encryption software. Virgin Media has stated that, following its own internal review, it has already implemented all of the requirements imposed on them by the ICO.

In other cases involving the loss of personal information, such as the theft of Ministry of Defence laptops and of a laptop from the home of the managing director of a company processing personal data on behalf of Marks & Spencer, the ICO has issued formal Enforcement Notices under the DPA. However, in this case, the ICO considered a formal undertaking to be sufficient in light of the remedial action already taken by Virgin Media and the company’s recognition of the severity of the matter. It warned, however, that any future breach will likely result in enforcement action. Similar undertakings have been entered into by organisations including Orange, the Department of Health and the Foreign and Commonwealth Office.

The Virgin Media incident highlights the costs of a breach of the data protection principles in terms of negative publicity, customer support and internal investigation. In the future, the costs have the potential to be even higher as the ICO was recently granted further enforcement powers enabling it to fine organisations where the DPA principles are breached either deliberately or knowingly or recklessly and in a way which is likely to cause substantial damage or distress. These new powers are not yet in force but their introduction suggests that any future loss of personal information can expect a robust response.
Disaster struck Deutsche Telekom AG when it lost 17 million sets of customer data in 2006. This was one of a number of data loss scandals involving the telecommunications giant which is T-Mobile’s parent company. Since announcing the data loss, Deutsche Telekom has pledged to boost its data protection efforts and has implemented a number of new measures. In November 2008, Philipp Humm (T-Mobile Germany’s Managing Director) took full responsibility for the data incidents and stepped aside from his post.

The lost data included names, addresses, phone numbers, dates of birth and email addresses. However, Deutsche Telekom told the press that “the records do not contain bank details, credit card numbers or call data.” The statement said that, “Deutsche Telekom has no evidence to confirm that the records have led to harassment of users in 2006 or subsequent years, or that they have otherwise been misused by unauthorised parties.”

Nevertheless, this is one of a number of incidents that has tarnished Deutsche Telekom’s image. In response to the incident, the company has intensified its security measures. A number of technical improvements have been made and high on the agenda has been improving password protection and creating greater access restrictions. According to the company, “access to databases managing customer data is being monitored closer than ever and registered.”

In addition to these technical improvements, there has been a reshuffle at board level. Dr. Manfred Balz has been appointed as the head of a new data privacy department which is also responsible for Legal Affairs and Compliance. Dr. Balz has taken on the supervisory function (which has been separated from operational responsibilities) and has a right of veto over all business decisions relating to customer data. The internal measures taken to improve data privacy are supplemented by a range of external measures. Dr. Balz plans “the establishment of a data privacy council to be made up of leading data privacy experts from independent organisations, academia and business.”

In reference to its previous security measures, Deutsche Telekom summarised the conclusions of an internal report in a press release which stated that, “the measures initiated by T Mobile in 2006 to recover the stolen data and to prevent its broader distribution, for example by quickly calling in investigative authorities, were correct, but that there were shortcomings in the subsequent organisational pursuit and processing of the case.”

The shortcomings referred to include allegations that call data was used inappropriately, subsequent to the company becoming aware of the data loss and whilst investigations were taking place. It was announced in October 2008 that “the five managers and employees who had operational or organisational responsibility in these cases have been suspended from their positions until further notice.”

To make matters worse, the company announced in October 2008 that a technical error had put the data of 30 million mobile phone customers at risk.
Confession time for telecoms companies?

If European law reform proposals are accepted then telecoms companies will be forced to notify authorities if they suffer a data breach. The European Parliament voted in favour of reform in September 2008 and although it decided against creating a super-regulator of telecoms, it agreed to make widespread changes after reviewing proposals from the European Commission.

The European Commission originally proposed a package of reforms in November 2007 designed to update privacy, data protection and telecoms laws. After making substantial amendments, the European Parliament accepted many of the proposals at the first-reading stage in September 2008.

The new rules will oblige telecoms companies to notify national regulators if there has been a data security breach that could pose a threat to privacy. In turn, the national authority would be obliged to report to the Commission, and would be required to submit an annual summary report detailing notifications received and action taken. Members hope that the changes will increase competition and provide consumers with clearer information.

On the Europa website, the European Commission “reaffirms the need of telecoms operators to notify regulators and the public about security breaches...” and that “notifications must, as a matter of principle, be sent to the individuals affected by them and that the notification procedure must remain swift, simple and effective.”

It seems that the notification requirement may be limited to telling authorities when the data in question is adequately encrypted. However, if the data is not suitably encrypted and the breach is considered serious, the provider will be required to notify individuals without delay.

The European Commission's original plan to create a super-regulator of telecoms has now been downscaled. The Commission clarified that the European Telecoms Authority "will be substantially smaller in size and competences than initially envisaged." Taking into account the wishes of Parliament and Council, the European Commission announced that the Authority "will be a lean and efficient office that will focus on telecoms regulation and have no competences with regard to spectrum or network security."

In November, the European Commission amended its proposals in light of the points raised by the European Parliament. The European Parliament is expected to have a second-reading of the proposals in April 2009.
Cisco recently commissioned InsightExpress (a US based market research firm) to conduct a global security study to investigate the prevalent issue of data security and leakage from within organisations and its potential link to employee behaviour.

Cisco suggests the security of information and the prevention of its leakage has its roots in the technology user’s behaviour. The aim of the study therefore was to identify how, by understanding employee behaviour, organisations could be better placed to tailor their risk management plans at local level, whilst at the same time ensuring that their business remains global in its nature and scope. The study was aimed to highlight to all organisations of every size and in every sector the need to understand these behaviours and how they can seriously affect the security of data by increasing or decreasing the possibility of a data loss incident occurring.

The survey was conducted to compare “employee behavioural risks” across various jurisdictions and cultures. It was also to take into account the different levels of reliance on technology and varying economies in these different countries. The study surveyed more than 2,000 employees and IT professionals from the United States, United Kingdom, France, Germany, Italy, Japan, China, India, Australia, and Brazil.

Ten key behavioural findings were identified by InsightExpress from the survey:-

- 1 in 5 employees altered security settings on work devices to access unauthorised web content. The study found that altering security settings on computers was a popular behaviour, with many employees feeling that they were entitled to look at what they want regardless;
- 7 out of 10 IT professionals said that employees accessing unauthorised applications (for example, iTunes) was the cause of up to half of the data losses their organisation had encountered;
- 2 out of 5 IT professionals have discovered employees accessing unauthorised parts of the networks or facilities in place;
- 24% of employees admitted to casually sharing sensitive information to family, friends and in some instances to complete strangers;
- 44% of respondents stated that they had shared their work issued devices with non employees without seeking permission from their employer;
- 50% of those surveyed send unauthorised emails to non employees, thus demonstrating that employees are unable to differentiate between work and personal lives as devices are used freely for both work and personal use;
- 1 in 3 employees admit to leaving computers logged on and unlocked, or leaving their laptops at their desks overnight, creating opportunities for theft and potential data loss;
- 1 in 5 employees have their login and password details written down on their desk;
- 22% (almost 1 in 4) carry business data on portable storage devices outside of the office increasing the opportunities for theft to occur or loss of devices by employees themselves;
- 22% of German employees are content to allow non-employees to roam their offices without any supervision (across the other countries surveyed the average was 13%). It shows that whilst the risks to data inside the office, as well as outside the office, is not guaranteed.

The results of this survey may be startling, or they may simply confirm the worst fears of many executives tasked with countering data leakage within their organisation. Cisco suggest that organisations take these survey results on board and consider the physical security of data and devices containing data as important as network security.

It is recommended that organisations should take adequate steps to know where the data they process is stored and how it can be accessed, used and by whom. Companies should take steps to educate employees on data protection issues and how they can impact upon an organisation’s finances (a particularly topical issue in the current climate).

In respect of international companies, the survey suggests that they will need to put in place global policies coupled with local policies, which can be bespoke to a particular country (depending on the financial and cultural circumstances in which the employees are working).
Google to anonymise search data after 9 months

In recent exchanges between Google and the Article 29 Working Party, Google agreed to anonymise search information within 9 months of collection but appeared to claim that the EU Directive on data protection does not apply to Google’s operations in Europe.

Google has recently been the subject of criticism from a number of bodies in relation to its retention of search information. For each search which is conducted via its search engine, Google collects the following information: the query; the time and date; IP address of the computer making the query; and the unique ‘cookie’ ID assigned to the computer. Google claims that this information is retained to improve the quality of search results, fight fraud and improve data security.

In a 2007 survey published by Privacy International, Google came bottom in a ranking of how internet companies handled customer data, based in part on the retention periods for searches and associated IP addresses. In April 2008, the Working Party stated that it was of the opinion that retaining this information for longer than 6 months was likely to be a breach of EU data protection laws.

Google originally retained search information for 18-24 months. This period was reduced in 2007 to 18 months.

Previously, Google had claimed that the retention of search information for longer than 6 months was justified by the effect of the European Data Retention Directive, which Google maintained placed the company under an obligation to retain information on the particular searches from IP addresses.

However, in September, Google accepted the Working Party’s contention that the Retention Directive did not apply to Google as it was an internet content company (i.e. the Directive only applies to telecom firms or internet access services) and therefore “the general obligation from the European Data Protection law is that the data must be deleted as soon as possible”.

On this basis, Google has agreed to further reduce the time for which search information linked to a particular IP address is held from 18 months to 9 months.

Google and the Working Party also disagreed on the question of whether the EU directive on data protection applies to Google at all. In its response to the Working Party, Google claimed that the sole data controller in respect of Google user personal data is Google Inc., the US parent “irrespective of where the data is collected or stored”. Google, therefore, claims that the processing of user personal data by Google entities based in Europe (such as in data centres based in Belgium) is only conducted by such entities acting as data processors on behalf of the US parent and is not therefore caught by the EU data protection regime. This is a questionable analysis and assumes that Google entities based in Europe have no scope for determining the purpose or means of processing the user personal data without reference to the US parent.

Google also rejected as “very far fetched” the Working Party suggestion that storing and accessing a cookie on the computer of a user based within the EEA was sufficient to ensure that the data protection legislation applied to the controller accessing the cookie.

Google did however accept that because a number of its data centres are located within the EU, the effect of Article 4(1)(c) of the Directive is likely to “bring Google Inc. within the scope of application of the national data protection laws of the countries where the data centres are based”. Google concluded that it “is committed to complying with EU data protection principles for the benefit of [users] in Europe.”
IP addresses and personal data: K.U. v Finland

Classifying IP addresses as personal data could have serious implications for search engines and many other electronic businesses, in particular, the personalised advertising business model of the Internet. Recent court decisions have not clarified the position, so businesses that log IP addresses should proceed with caution.

An IP address is a device’s (typically a computer’s) address as expressed in the numerical format specified in Internet Protocol, IPv4, (24 digits) or IPv6 (128 digits, which increased the number of IP addresses available). An IP address is allocated by an Internet Service Provider (ISP) to ensure that data requested returns to the right place. There are two different types of IP addresses, namely dynamic and static. Dynamic IP addresses can change each time a connection to the Internet is made, while static IP addresses are reserved and do not change over time. Residential Internet connections, whether broadband or dialup usually use dynamic IP addresses, while commercial leased lines and servers have static IP addresses, so they can always be reached at the same address. For instance, the IP address for www.news.bbc.co.uk is always 212.58.226.75. Typing the numbers into a browser address bar will display the same result as typing the words.

In K.U. v. Finland, the European Court of Human Rights (ECHR) has decided to hear a potentially significant case considering whether victims of online activity may have a right to identify the internet users alleged to be responsible. In this case an unknown person placed an online solicitation for a sexual relationship under the name of a 12 year old boy, listing the boy’s name, phone number, date of birth and a picture. A second person contacted the boy and was later identified and prosecuted for it. The notice was taken down but the publisher of the notice remained unknown, except for his or her dynamic IP address at the time the notice was placed. The victim tried to identify the publisher – with the help of law enforcement – through the ISP that had issued the dynamic IP address. At that time, however, Finnish law did not give the police the authority to order the ISP to hand over the data to the police, because of the low punishment for the crime of acting under a fake identity. Finnish courts affirmed this impossibility. The complainant claims Finnish law does not give him an effective remedy under the ECHR with regard to an infringement of his private life.

The outcome of the case could have far-reaching effects on the privacy of all European Internet users, if it concludes that there was an actual infringement of the applicant’s right to private life. Importantly, Article 8 ECHR places Finland under a positive obligation to ensure the respect to private life between private parties. A ruling requiring contracting states to provide for the disclosure of IP addresses by ISPs would make further inroads into the ability to remain anonymous on the internet.

Karen McCullagh
Solicitor, Lecturer-in-Law, Salford Law School
Email: k.mccullagh@salford.ac.uk
German Court rules that IP addresses are not personal data

A German court has ruled that internet protocol (IP) addresses are not “personal data”.

IP addresses are the unique identifiers that are assigned to computers and other devices when they are connected to the internet. The data protection issue is to what extent can the IP addresses be linked to an individual by internet service providers (ISPs) or third parties and thus revealing an individual’s browsing history and their use of the internet?

In response to a claim by an individual that a web publisher’s storing of IP addresses was a use of personal data which breached German data protection law, the district court in Munich held that IP addresses do not have the required level of “determinability” to be personal data. They considered that the identity of the person from the IP address can not be established without disproportionate effort. The court held that the IP addresses could be stored without breaching an individual’s privacy rights under German law.

There has been considerable discussion across Europe in recent years as to the applicability of the Data Protection Directive to IP addresses when held by ISPs or website operators.

A distinction has been drawn by a number of authorities between “static” and “dynamic” IP addresses: a static IP address being one that remains the same whenever a particular computer links to the internet, a dynamic IP address being that changes each time a computer links to the internet.

The UK Information Commissioner issued guidance in 2007 that, when held by website operators, dynamic IP addresses can not be personal data because they can not be linked (other than by the ISP) to a particular individual. However, for static IP addresses, the Commissioner noted that if these are linked by an ISP or a website operator to a particular individual and/or used to build a profile of a user, such static IP address is capable of being personal data.

The Article 29 Working Party takes a wider view of dynamic IP addresses held by ISPs. In the Article 29 Working Party’s opinion, dynamic IP addresses are capable of constituting personal data. The Article 29 Working Party considers that it is still within an ISP’s “reasonable means” to “identify internet users to whom they have attributed [dynamic] IP addresses”. This is particularly the case where the IP address is being used to identify a particular individual (for example, in cases of copyright infringement arising out of file sharing). Therefore, the Article 29 Working Party considers that it is best practice for an ISP to assume all IP addresses are personal data.

Rules for social networks agreed by data protection authorities in Germany

The German Düsseldorfer Kreis, a panel gathering all German data protection authorities, has sent a clear message to social networks on the mandatory respect of the data protection legal framework and highlighted eight central requirements to respect.

Social networking services are on the rise globally, with potentially 243 million users they are the communication tool of choice for many young people with the most popular sites being Facebook, MySpace and Bebo. Social networking sites by their very nature expose a number of privacy issues, for example, uploading photographs containing third parties’ data, “referring a friend” applications, the quantity and control of personal data entered onto profile pages and the fact that these sites often operate internationally.

continues on page 20...
The kind of social networking sites offered by Facebook and MySpace allow an individual user to create their own personal profile and become friends with other users of the site (subject to that person accepting the “friend invitation”). Users can upload and share photographs and post messages on each other’s profiles. These sites usually have some kind of privacy control built in (although it is often at the option of the individual user to define their own privacy settings).

These social networking sites raise revenue through advertising and do not charge money for their membership.

Concerns have been voiced in relation to the quantity of personal data included on the sites, and the perceived threat that large corporations or government bodies may be able to access such information and personal profiles to use in decisions relating to that individual. Whilst it may be an exaggerated concern of privacy advocates, it has been reported that employers have searched the sites to view profiles of potential employees as part of the recruitment vetting process and organisations use the data as a method of targeted advertising. There is also concern that people using the site are not aware of the risk of data theft or viruses from the site.

Recently in Germany the German Dusseldorfer Kreis, a panel of the regional data protection authorities laid down 8 principles in relation to the operation of social networking sites designed to keep them in line with data protection laws.

The principles of operation include the following requirements:

• the sites only store information from a user’s profile if it is needed for billing purposes;

• information contained on the site can only be used for marketing if consent is obtained;

• an individual user must be able to delete their profile from the site; and

• social networking site operators need to adequately protect private information by putting in place technical security measures which set standard privacy settings to protect users’ privacy.

Whether these principles or something similar will be adopted in the UK will remain to be seen. As society becomes more aware of the privacy issues posed by social networking sites the desire for regulation and intervention may increase. The Information Commissioner has published guidance on the safe use of social networking sites and the Home Office (prompted by the use of the sites by underage individuals) has published guidelines for social networking site operators to encourage better practices. The key message is the need to make users of social networking sites more aware of the issues surrounding privacy and how they can protect themselves on these sites.

Privacy chief approves of sharing criminal records if privacy beefed up

Europe’s privacy watchdog, the European Data Protection Supervisor (EDPS), has given its backing to controversial proposals to share personal information between police forces across Europe despite strong criticism of the idea when the concept was first raised in April 2007.


The proposal is for a system which facilitates the exchange of information on past criminal convictions between Member States. Its main aim is to ensure that Member States are able to provide accurate and comprehensive responses to requests for information concerning its nationals from other Member States. Previously, national courts of Member States frequently passed sentences on the sole basis of past convictions appearing on their own national databases.

The proposal puts forward in May does not establish a European database of criminal records, but rather a system of interaction and cooperation between Member States’ criminal records systems and databases. The proposal sets out the general architecture for the exchange of information, laying the foundations for the future IT developments related to the interconnection of national criminal records.

Originally concern centred on whether the proposal would lead to the creation of a pan-European database which would hold sensitive personal data on citizens from all Member States of the EU. The EDPS was particularly concerned with such a scheme as it was unclear who would be responsible for that information. However, following a consultation, the EDPS has given the new proposal a positive but guarded response.

The EDPS has said the planned system to connect the criminal records databases of Member States is a good idea in principle provided that the data protection regime around it is sufficiently strengthened.

In particular, the EDPS has stated that “In Article 6 [of the Framework Decision establishing the ECRIS] reference must be made to a high level of protection as a precondition for all the implementing measures to be adopted. The EDPS supports the present proposal to establish ECRIS provided that the observations made in the present opinion are taken into account”.

The EDPS has also called for clarity as to who would operate the system itself. The EDPS considers that the Commission should be responsible for software connecting the databases and not individual countries.
The European Union Data Retention Directive was passed in January 2006. It orders all EU member states to pass laws requiring communications service providers to retain phone and internet data for between six and twenty four months. The Directive was introduced so that these records could be used by authorities when investigating crime.

Ireland agreed with the substance of the Directive, but objected to the European Union passing a Directive in areas of crime and security. They argued that the purpose of the EC Treaty was to harmonise national laws and improve the functioning of the internal market and that this does not extend to implementing provisions affecting serious crime. They reasoned that the Directive was inappropriate because it concerned police and judicial co-operation in criminal matters between the member states. The Irish government therefore filed a challenge before the ECJ in July 2006.

In October 2008 the Advocate General Yves Bot published his opinion on this matter. Although the Advocate General’s opinion is only advisory, it is followed in around 80% of cases by the ECJ.

The Advocate General believed that the Directive helped reduce a real risk of countries adopting different standards and requirements in the field of data protection. He stated that crime and security were an aspect of the internal market, and that the Directive assisted the development of the internal market for electronic communications by providing common requirements for service providers.

He also argued that the Directive explicitly gives member states the freedom to make their own decisions about what to do with the information held by telecoms companies and how to govern authorities’ access to it.

His opinion therefore concluded that the implementation of the Directive was appropriate under the EC Treaty.

The ECJ’s decision on this matter is expected early this year.

Ireland has in fact introduced more restrictive laws than suggested by the Directive. Whereas the Directive suggests countries order telecoms providers to keep data for between six and twelve months, Ireland’s data retention laws require telecoms firms to keep data for three years.

The UK has implemented parts of the Data Retention Directive. The Data Retention (EC Directive) Regulations 2007 came into force on 1 October 2007 and mandate the retention of non-internet data. These Regulations are expected to be replaced on 15th March 2009 by a wider set of rules that extend the current regime to cover internet data as well.
The Article 29 Working Party (an independent European advisory body on data protection that comprises data protection officials from EU member states) has developed a toolkit to help global companies comply with EU laws that control overseas transfers of personal data within their groups. The toolkit encourages the use of Binding Corporate Rules (BCRs).

The Data Protection Directive prohibits the transfer of personal information to countries outside the European Economic Area (EEA) unless there is adequate data protection in place. Some non-EEA countries are recognised as having adequate data protection, including Switzerland, Canada, Argentina, the Isle of Man and Guernsey. Transfers to these countries are therefore lawful. For transfers elsewhere, adequacy must be ensured by other means, for example, by obtaining the consent of the data subject or by the use of European Commission authored model contractual clauses. Another, less popular means of compliance is the use of BCRs. BCRs are designed as an alternative to two existing schemes for the transfer of data: Safe Harbor and the model contract clauses. Safe Harbor is a scheme which pre approves select US organisations as organisations to which EU based organisations can transfer data. Model contract clauses (drafted by the European Commission and approved by the Information Commissioner’s Office) can be used by EU based organisations as a way of ensuring that the transfer complies with privacy law.

The BCRs on the other hand were created by the Article 29 Working Party (Working Party) to allow companies to send data to other parts of the organisation or to a group company located in countries outside the EEA and whose data protection regime has not been designated as adequate. A multinational company can adopt BCRs (effectively a binding code of corporate conduct). However, each company must devise its own BCRs and have them approved by the data protection authority of every EU country in which they will be used.

The BCRs proved unpopular and therefore in 2005 the Working Party published a model checklist describing the required contents of an application for BCR approval. They still however failed to win support. At the time of writing, the UK Information Commissioner’s website lists just two companies with approved BCRs: General Electric and Philips.

The Working Party has now developed what it describes as a toolkit, to encourage the adoption of BCRs. The new set of documents aims to help companies formulate their BCRs. The toolkit includes a framework document which outlines how BCRs should be structured and what they should contain. It also provides a helpful table checklist of what must be presented to data protection authorities in the BCR application.

The Working Party has warned that companies must not simply copy the framework document and pretend that it is a full policy. They state:

"[Data protection authorities] will not accept a pure copy and paste of this framework... This framework for BCRs is not a model BCR it is just a suggestion of the content and how the rules might be structured in a single document which can be made binding on the group of companies. BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake and the policies and procedures that they have in place to protect personal data."

The Working Party produced the documents to help companies understand and implement the protections for transferred data. According to the Working Party, European Data Protection Authorities had found that international companies interested in BCRs did not have an exact understanding of the structure of BCRs and that they were concerned by the length of the approval process. Further, they found that most data protection authorities do not have enough staff dedicated to BCRs. Together these factors appear to have contributed to the lack of use of BCRs.

In light of this, the Working Party has updated its guidance. The toolkit seeks to address important issues for companies looking to put BCRs in place and to tackle some of their frequently asked questions. These include, for example, the circumstances in which BCRs should be used, who is liable for breaches of the rules, and the rights of those whose data is transferred under the rules.
In April 2007, the personal details of 380,000 social welfare recipients were lost as a result of the theft of a laptop computer belonging to the Comptroller and Auditor General’s office. In April 2008, Bank of Ireland informed the Irish Data Protection Commissioner that four laptops containing the details of over 31,000 customers had gone missing between June and October 2007. There was also discovery of patient records in a disused landfill, relating to patients treated at Cork Regional Hospital (now known as Cork University hospital) and St. Finbarr’s hospital.

The Minister for Justice, Dermot Ahern, indicated that the review should look at whether any changes should be made to the legislation to provide greater protection to personal data. The legislation governing data protection in Ireland is the Irish Data Protection Act 1988, as amended in 2003 by the Data Protection (Amendment) Act. This Act incorporates Directive 95/46/EC into Irish law.

In particular, the review group will consider whether organisations should be subject to a statutory obligation to report security breaches and will also look at whether fines should be imposed. The group will take into account approaches to this issue in other countries and will assess the regulatory and economic impact of making changes to the law.

In Ireland, as in the UK, there is currently no mandatory requirement to report a security breach to the regulator. One of the concerns expressed by the UK Information Commissioner is that if tiny breaches were reported regularly, it could create an impossible workload. It will be interesting to see what conclusion the Irish review group will reach in relation to this issue.

The Irish Minister for Justice said in relation to the proposed review group:

“In our modern society, the services and facilities we avail of increasingly involve the recording of our personal data by both private and public bodies.

“Given recent experiences, there is an understandable concern in the public mind at reports of such data being lost or mismanaged.

“Various suggestions have been made as to how data protection legislation ought to be amended to address these concerns, and I intend to get a broad assessment of these complex issues and the possible impact of any changes, taking account of the international experience, where a variety of approaches have been attempted.”

Mr. Billy Hawkes, the Irish Data Protection Commissioner, will be a member of the group, which will be chaired by Mr. Eddie Sullivan, the former secretary general at the Department of Finance. Interim recommendations will be made by the review group if they consider it appropriate to do so.
ANALYSIS:

Data Protection Compliance in Israel’s Pension Fund Industry Reform

Yoram Hacohen* & Omer Tene**

In the summer of 2005, Israeli banks were mandated to divest their holdings in pension funds and mutual funds, as part of a set of reforms intended to reduce concentration in the financial market. Consequently, the banks sold their holdings in pension funds to insurance companies and other investment vehicles. The ensuing series of transactions, of significant scale and scope relative to the size of the Israeli market, raised a host of data protection issues requiring regulatory resolution. In this article, we introduce several questions and dilemmas which arose from the regulatory review of the divestitures and acquisitions in Israel’s pension fund industry.

Regulatory Cooperation

Interestingly, the data protection regulator, the Israeli Law and Information Technologies Authority (ILITA), came to scrutinise the transactions as a result of requests of the purchasers to change the details of the databases’ registration status. These requests, in turn, were motivated by the instruction of financial market regulators, who provided the parties with a check list of regulatory assignments to be completed prior to the authorization of the transactions. This process underlines the importance of cooperation among regulatory agencies. By integrating privacy considerations into their regulatory frameworks, telecom, financial market and consumer protection regulators may help weave a regulatory web ensuring compliance with data protection law.

Israeli Data Protection Law

The right to privacy has been elevated to constitutional status in Israel in Section 7 of Basic Law: Human Dignity and Freedom of 1992. Dating from 1981, Israel’s Privacy Protection Act (PPA) is one of the first data protection statutes in the world. Under the PPA, databases containing “sensitive data”, defined as \textit{inter alia} information about an individual’s financial condition, are subject to mandatory registration with the Database Registrar, which is currently a unit of ILITA. Section 9(b) (2) of the PPA provides that the controller must specify in its registration application “the purposes for which the database was established and for which the data are intended”. Section 10(a)(2) of the PPA authorizes ILITA to “register a database with a purpose different than the one specified in the application, register several purposes, or order the controller to file several applications in place of the one filed, if such modifications better reflect the actual use of the database”. Any post-registration change in the identity of the controller or the purposes for which the data are intended must be notified to ILITA under Section 9(d) of the PPA.

Section 11 of the PPA requires controllers to provide data subjects from whom data are collected information concerning the purposes for which the data are intended, any recipients of the data, and the purpose of any data transfer. The purpose limitation principle is set forth in Section 2(9) and 8(b) of the PPA, under which the use or transfer of personal data for a purpose other than that for which the data were provided constitutes an invasion of privacy. An invasion of privacy is both a civil tort and a criminal offence.

* Head of the Israeli Law and Information Technologies Authority; ilita@justice.gov.il.
** Israeli legal consultant; Associate Professor, College of Management School of Law; omer.tene@bezeqint.net.
1 The Bachar Reform, named after Dr. Yossi Bachar, Director General of the Ministry of Finance, who led a government committee charged with the restructuring of the financial market, resulted in the enactment of the Increasing Competition and Reducing Concentration and Conflicts of Interests in the Israeli Financial Market (Legislative Amendments) Act, 2005; Regulation of Financial Services (Pension Funds) Act, 2005, and the Regulation of Financial Services (Pension Advice and Marketing) Act, 2005.
Members’ consent to the transfer

An initial question that arose from the sale of the pension funds’ assets was whether the transfer of a database containing information about the fund members’ financial condition requires such members’ prior consent. Needless to say, the banks and insurance companies wanted to perform the transactions without having to solicit consents. Yet under the PPA, data transfers to third parties, including corporate affiliates, may constitute a breach of the purpose limitation provisions, absent such consent. Under Section 11 of the PPA, any prospective transferees must be notified in advance to the data subjects. It is not clear, however, if consent is required under the PPA where a transfer does not alter the initial purpose for which the data were collected. In addition, the parties could have relied on Section 18(2)(b) of the PPA, which exempts form liability privacy infringements that were mandated by a legal obligation, in this case financial reform legislation. ILITA concluded that specific consent is not required to effectuate the transfer of a database between pension fund management companies. ILITA reasoned that the transactions were mandated by statute and that fund members were granted an opt-out option to transfer their savings to a different fund if they were dissatisfied with the incoming management company.

The controllers

The pension fund purchasers sought to register the parent entity of the insurance group as data controller. This would facilitate intra-group data transfers, integration of data into a central database and potential expansion of the legitimate uses of data. The purchasers pointed to the economic structure of the acquisition, which typically featured the parent company, as opposed to the pension fund management company, executing the transaction. ILITA rejected this approach and required pension fund management companies (fund managers), which are lower down the corporate hierarchy, to register as controllers. ILITA relied on pension fund regulation, which imposes duties of care and loyalty on fund managers, as well as on data protection law, which restricts uses of data to those authorized by data subjects. ILITA exercised its authority under Section 10(a)(2) of the PPA, to mandate separate registration of each fund’s database under the name of that fund’s management company. It explicitly stated that the consequence of separate registration is that insurance groups operating more than one pension fund may not integrate members’ data into a central database without such members’ prior consent. ILITA stressed, however, that the restrictions on data transfers do not reflect on the economic ownership of the pension funds. Thus, while a pension fund’s database must be locally controlled by its management company, the fund’s assets may be managed centrally by the insurance group’s parent company.

The processors

Under the acquisition agreements, despite divesting their holdings in pension funds, banks would continue to provide fund purchasers with data processing services. This is due to the technical expertise and IT systems developed by the banks over the years. The banks argued that as sellers and/or data processors, they may continue to lawfully use the funds’ databases for their own business purposes. ILITA held that while fund managers may authorise banks to act as data processors on their behalf, they may do so strictly for the purpose of operating the funds for their members’ benefit. Any additional use of the data by the banks is strictly prohibited. Consequently, the banks were ordered to comprehensively map the information flows in their system and delete and avoid use of any copy of the pension funds’ data, except in connection with the provision of processing services to the purchasers. Under Section 10(b)(3) to the PPA, the banks were required to verify the deletion of the data by an affidavit. However, ILITA recognized that the banks may have a legitimate interest or even a legal obligation to retain certain data and documentation for potential use as evidence at trial. In these limited circumstances, banks would be permitted to lawfully retain the data, provided that they would not be used for any additional purposes. Finally, ILITA instructed the purchasers to verify the processors’ compliance with data security requirements under Section 17A of the PPA.

An additional argument raised by the banks in this respect was that the pension fund members initially granted their consent to use the data for both the operation of a pension fund and the provision of pension advice. The Bachar Reform required banks to terminate the former activity but
not the latter. Hence, banks claimed that despite the sale of the pension funds, they were entitled to continue to use the funds’ databases in order to provide members with pension advice. ILITA rejected this argument, holding that the transfer of a database from a controller to a third party has the effect of “resetting” the data subjects’ consent. The transferor cannot maintain a “portion” of the initial consent. The data subjects’ consent hinges on a specific database, and once that database is sold, the consent is “transferred” with it. ILITA reasoned that any other interpretation would allow parties to duplicate data subjects’ consent time and again by transferring the database.

The purpose of the database

ILITA determined that the purpose clause in the funds’ database registrations must state that “the database will be used for the lawful managing, operation and marketing of a pension fund”. ILITA exercised its authority under Section 10(a)(2) of the PPA to reject attempts to register broader purpose clauses. It held that the databases may be used strictly to perform tasks allocated to fund managers under pension fund regulations; such as accounting for deposits and withdrawals, managing fund assets, preparing periodic reports, and marketing services of the pension fund itself to the members. ILITA held that the purpose clause marks the boundaries of the members’ implied consent to the processing of their personal data upon joining a pension fund. ILITA rejected fund manager claims to legitimise additional uses of data, particularly for marketing purposes or the provision of direct marketing services to third parties.

Direct marketing by fund managers

Substantial legal controversy revolved around the extent of lawful use by fund managers of members’ personal data for direct marketing purposes. Insurance groups offer a broad array of insurance and financial products, which they are eager to market to existing customers. In addition, third parties seeking to market their own goods and services found great interest in the extensive financial data held in pension fund databases. Besides the purpose limitation provisions of Section 2(9) and 8(b) of the PPA, such marketing activities are subject to Subchapter B of Chapter B of the PPA, governing direct marketing, and to the recent amendment to the Telecommunications Act, governing unsolicited communications via electronic means.²

ILITA approached these questions by making several factual distinctions. It distinguished between marketing (a) services that are substantially equivalent to pension savings or other goods and services; (b) by the fund manager, a member of the insurance group or a third party; (c) with or without an actual data transfer; (d) based on specific profiles or categories of data or to the customer list as a whole. The result of these distinctions is a matrix delineating the lawful uses of data for direct marketing services in the pension fund sector.

The relatively simple case is where the fund manager itself approaches its members to market its own products. Such approach is permitted, provided that the fund manager complies with the direct marketing provisions of the PPA, which include an opt-out right for data subjects.³ At the other extreme is a transfer of data from the database to a third party for direct marketing purposes, an activity defined in the PPA as “direct marketing services”.⁴ Such a transfer is prohibited without the data subjects’ prior informed consent and without registering direct marketing services as one of the purposes of the database.

More complex are the situations in between the two extremes, such as where the fund manager provides direct marketing services to a third party without transferring actual data (e.g., host mailing). After careful deliberation, ILITA held that in order to balance the competing interests of controllers and data subjects, it would allow direct marketing services to third parties, provided that all of the following conditions are met: (a) the approach must not be based on profiling or segmenting but rather to the customer base as a whole; (b) the marketed product must be a pension

---

² Amendment No. 40 to the Telecommunications Act (Telephone and Broadcast) 2008, adding Section 30A to the statute.
³ Section 17F(a)(2) of the PPA.
⁴ Section 17C of the PPA.
product as defined by pension regulations; (c) the third party must be a corporate affiliate of the fund manager; and (d) the fund manager must comply with the direct marketing provisions of the PPA, including proper notice to the data subjects and provision of an opt-out right.

ILITA emphasized that its opinion does not derogate from the new provisions of the Telecommunications Act concerning unsolicited communications, which are not subject to its regulatory authority. Under the recent amendment to the Telecommunications Act, unsolicited communications to individuals via electronic media require affirmative opt-in consent, with a “soft opt-in” exception for existing customers.

**Conclusion**

The regulatory oversight of the divestitures and acquisitions in Israel’s pension fund industry highlighted the importance of addressing data protection concerns when performing significant economic transactions. From a regulatory perspective, engaging a set of transactions such as the pension fund sales creates a positive externality, by raising data protection compliance to the attention of dominant actors in the financial sector as well as leading law firms. Hopefully, with increased awareness and the involvement of legal professionals, increased compliance will come.

The fluid, replicable nature of data raises the difficulty of controlling their use or verifying their deletion subsequent to a business sale. In addition, the data protection objective of purpose limitation must be balanced in these cases against the legitimate interest of the seller to retain copies of the data as evidence in potential prospective litigation.

Upon close scrutiny, significant mergers and acquisitions may turn out to be motivated by the use of personal data. In these cases, data protection regulators should try to identify the correct balance between enforcing data subjects’ privacy rights and facilitating legitimate economic activity.

This article was originally published in Data Protection Law and Policy in November 2008 by Cecile Park Publishing.
ANALYSIS:

Government Information Assurance Agenda

CONTENTS AT A GLANCE

The functionality, accessibility, security and reliability of information are key assets in the delivery of public services by the Government. In recognition of this and in order to facilitate the sharing of information across departments, the Government commissioned two reviews. The first was part of the National Information Assurance Strategy, which was initially published in 2007 by the Cabinet Office, and focused upon establishing the following objectives:

• Effective risk management
• Appropriate information assurance standards
• Appropriate information assurance capabilities

Its ultimate aim was to establish "a UK environment where citizens, businesses and government use and enjoy the full benefits of information systems with confidence" by 2011.

This was followed by an independent review on how well the Government was performing with regard to information assurance. Its findings were released as the Coleman Report in June 2008. Although it recognised that there were improvements in attitudes towards information security, in terms of money and effort, there was criticism in the following areas:

• Performance standards
• Policies to monitor and respond to risk
• Training of staff
• Internal reviews

The Government responded by implementing a key number of the recommendations from the Coleman Report. However, the main feature of the Coleman Report was the need to adapt to technological developments and provide a more integrated operation of information assurance, and this is a matter for constant review.

What is “information assurance”?

Information assured ensures the confidentiality, availability and integrity of electronically held information.

Information inputted into a computer enters the electronic domain and from thereon can be changed, deleted or broadcast to the world. Electronic information must be readily available when required and reliance may be placed upon its accuracy. Information assurance is defined by the Government as confidence that information systems will protect the information they carry and will function as and when required under the control of legitimate users. The purpose behind information assurance is to ensure that the confidentiality, availability and integrity of all electronically held information is sufficiently maintained and upheld.
Re-visiting the Government’s National Information Assurance Strategy

Information assurance activity across the UK is monitored by the Central Sponsor for Information Assurance (CSIA), which is a unit within the Government’s Cabinet Office. The CSIA produces and maintains the National Information Assurance Strategy (NIAS), which is a guide to assist the Government in achieving the following strategic outcomes:

- to make central and local Government better able to deliver public services through the appropriate use of information and communications technology (ICT);
- to strengthen the UK’s national security by protecting information and information systems at risk of compromise; and
- to enhance the UK’s economic and social well-being as Government, business and citizens realise the full benefits of ICT

The NIAS was initially published by the Cabinet Office in 2003. It recognised that ICT is a critical asset for any organisation and that information assurance is important in the delivery of public services. Government Departments became committed through the Transformational Government agenda to change the provision of public services through ICT. The NIAS was thereby updated in 2007 in response to technological developments in ICT and to keep in line with Government policy.

The adapted NIAS envisioned by 2011 a UK environment where citizens, businesses and Government use and enjoy the full benefits of information systems with confidence.

It was proposed that information risk management can be controlled through compliance with standard protocol and by ensuring the right level of professionalism, education and training. The following three approaches were recommended, which have important implications for the way organisations, particularly within Government, do business:

- Clear and effective information risk management by organisations
  - Clear board-level ownership and accountability for information risks will be required;
  - Where information is shared, a single point of risk ownership will be identified.

- Agreement upon and compliance with approved and appropriate information assurance standards
  - Organisations, particularly those within, or linking to the Government, will operate within a national framework of information assurance common standards;
  - Trust and confidence in the use of information will be maintained through an effective model of compliance with these standards.

- The development and availability of appropriate information assurance capabilities
  - The Government will work more closely with wider sectors in the development of “capabilities” to enable organisations to manage information risks;
  - These capabilities include: availability of the right products and services; coordinated and appropriate efforts on innovation and research; improved professionalism, and awareness and outreach.

The approach determined by the NIAS is developed from an understanding of the threats to UK ICT. Threats to information assurance encompass not only attack risks such as e-crime, ID fraud and theft, but also the greater vulnerabilities associated with the increase in the pace of ICT development and the risks of operating in a global marketplace.

The strategy identifies the following benefits to the public sector of embedding information assurance in its use of ICT:

- reducing the risk of potential financial, reputational and operational damage to organisations from the growing risk of compromise to ICT; and
- ensuring that public sector departments will get the most appropriate and best value information assurance products and services.
It also identifies wider benefits to the private sector and the general public, as set out below:

- ICT and information assurance industries will benefit from more timely, relevant and valued engagement with Government;
- the wider private sector and the Government will benefit from sharing best practice for information assurance and the management of information risks; and
- citizens will benefit from safer access to e-enabled public services and an improved awareness of how to protect their own electronic devices.

The Coleman Report

The Cabinet Office commissioned an independent assessment of Government departments’ information assurance practices by Nick Coleman, former head of IBM’s security services division in Europe, Middle East and Africa.

The review was asked to report back on:

- whether information assurance across Government is adequate enough to provide stakeholder confidence in the Government’s information infrastructure;
- whether information and services are protected in a timely and cost-effective way; and
- the extent to which current investment in information assurance will support the requirements of shared services and the Transformational Government agenda.

Key recommendations from this work were actually published in a synopsis in June 2007 in order to be able to inform the direction of the NIAS delivery plan and the full report was published in June 2008. On the issue of data security the Coleman Report was updated to reflect the O’Donnell review Data Handling Procedures Across Government: Final Report which was also published in June 2008.

The consultation process was undertaken over eighteen months, considered departments and agencies across Government and other areas of the public sector, and focussed on all elements of information assurance: data protection, availability and the integrity of information.

The report identified that most departments are now investing significant amounts of money and effort in information security.

The Government needs to be able to demonstrate a comprehensive understanding of the risks it is facing and needs to put in place clear policies that mitigate the risks.

The report identified that most departments are now investing significant amounts of money and effort in information security. It was found that there are areas of good practice, but there are also many areas where Government must improve.

It stressed that the Government must do more to deliver confidence in its information infrastructure by enhancing governance, information risk management policy and monitoring. At present each individual departments has developed its capabilities independently and this has resulted in unnecessary complexity with many different areas of Government addressing the same challenges differently. Coleman believes the challenge is to enable joined up Government, which means sharing more data and services across departments.

Coleman recommended that strategically the Government needs to be able to demonstrate a comprehensive understanding of the risks it is facing and needs to put in place clear policies that mitigate the risks. Further it needs to monitor performance for compliance and ensure that there is capacity to respond to incidents. The report lists ten elements necessary for successful information assurance and makes the following recommendations for the Government in respect of these elements:

- Set out acceptable parameters for the sharing, management, and protection of information held and managed by Government.
- Create new mechanisms, including a central facility, for reviewing and managing information risks across Government for information sharing.
- Annual audit of departments’ capabilities and quarterly reports on information risks and performance.
- Provide the Prime Minister with a summary of information assurance across Government and associated spending required to deliver cross Government information security.
• Enable one central mechanism for developing coordinated joint working, sharing best practice and establishing information assurance priorities across departments and agencies.

• Create mandatory policy rules on security across Government to define minimum department standards and enable compliance monitoring.

• Mandate the use of privacy impact assessments to tackle identity management challenges.

• Ensure education on information assurance and mandate professional certification for those working in information assurance in key defined roles across every Government department.

• Measure security through audit and monitoring to a defined standard. Report incidents to an independent organisation to investigate.

• Have an independent oversight capability retained by Government who can be called upon to give independent advice on information assurance.

The Government’s response

A ministerial statement was published on the same day that the Coleman Report was released and set out minimum mandatory standards for Government departments to comply with which include:

• introducing new rules on the use of protective measures, such as encryption and penetration testing of systems;

• standardising the processes by which departments understand and manage their information risk, identifying the key individuals responsible for information assets and setting out their responsibilities;

• requiring quarterly risk assessments within each department on the confidentiality, integrity and availability of information;

• introducing mandatory training for all staff involved in handling personal data;

• requiring the use of Privacy Impact Assessments when introducing new policy or processes that involve the use of personal data;

• introducing greater scrutiny and monitoring through the inclusion of information risk in Statements on Internal Control, which are scrutinised by the National Audit Office and through spot checks by the Information Commissioner; and

• enhancing transparency of arrangements, through annual reporting to Parliament on progress and the use of Information Charters which provide clarity to citizens about the use and handling of personal data.

Verdict

The NIAS was criticised by some quarters of the media for recycling old ideas and for being a late response to discussions and proposals in respect of information assurance in the preceding years, such as the Information Assurance Advisory Council strategy.

In essence the Coleman Review finds that information assurance is progressing within Government departments; but stresses that in a joined up world, where data and services need to be connected and layers of trust need to be established, new thinking and new mechanisms need to be put in place. There is direct criticism of the current procedures; for example when discussing accountability the review finds that “no role exists to provide Independent Oversight that the appropriate Governance; Information Risk Management; Policy and Operations; and Monitoring and Controls around information assurance are in place across departments and agencies.” Risk assessment is stated to be “patchy leaving many without a clear understanding of the risks they are facing or exposing their stakeholders to”.

As well as the Coleman Review, in recent times the Poynter Report, the Independence Police Complaints Commission Report, the Burton Report, the Cabinet Secretary’s Data Handling Review and the Thomas/Walport Report into data sharing have all been published in the aftermath of a number of well publicised security lapses in the public sector. The Coleman Review indicates that the NIAS leaves gaps that need to be filled and in the current climate the importance of addressing the issues raised by information assurance is enhanced.
Details of the content of Amberhawk’s data protection and FOI courses, a course bookings form and other comprehensive details (e.g. costs, discounts) can be downloaded from the Amberhawk web-site, www.amberhawk.com or by contacting info@amberhawk.com (telephone: 0845 680 2623).

Attendance at all courses D1-D7, DN1-DN5, F1-F7 and FN1-FN5 covers the ISEB syllabus in data protection or FOI.

### Dates of Data Protection Courses in London

<table>
<thead>
<tr>
<th>CODE</th>
<th>Dates</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>D1</td>
<td>13th January 2009</td>
<td>21th April 2009</td>
</tr>
<tr>
<td>D2</td>
<td>14th January 2009</td>
<td>22th April 2009</td>
</tr>
<tr>
<td>D3</td>
<td>27th January 2009</td>
<td>12th May 2009</td>
</tr>
<tr>
<td>D4</td>
<td>28th January 2009</td>
<td>13th May 2009</td>
</tr>
<tr>
<td>D5</td>
<td>10th February 2009</td>
<td>2nd June 2009</td>
</tr>
<tr>
<td>D6</td>
<td>11th February 2009</td>
<td>3rd June 2009</td>
</tr>
<tr>
<td>D7</td>
<td>10th March 2009</td>
<td>16th June 2009</td>
</tr>
<tr>
<td>Mock</td>
<td>24th March 2009</td>
<td>1st July 2009</td>
</tr>
<tr>
<td>DTutorial</td>
<td>3rd April 2009</td>
<td>8th July 2009</td>
</tr>
<tr>
<td>Exam</td>
<td>24th April 2009</td>
<td>17th July 2009</td>
</tr>
</tbody>
</table>

### Dates of Audit and Update Events in London

<table>
<thead>
<tr>
<th>CODE</th>
<th>Dates</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>DU</td>
<td>26th January 2009</td>
<td></td>
</tr>
<tr>
<td>D8</td>
<td>17th February 2009</td>
<td>21st July 2009</td>
</tr>
</tbody>
</table>

### Dates of Two Day “Secure and Lawful Information Assurance” in London

- 24th and 25th February 2009
- 14th and 15th May 2009
## DATES OF DATA PROTECTION COURSES IN MANCHESTER

<table>
<thead>
<tr>
<th>CODE</th>
<th>DATES</th>
</tr>
</thead>
<tbody>
<tr>
<td>F1</td>
<td>30th April 2009</td>
</tr>
<tr>
<td>F2</td>
<td>1st May 2009</td>
</tr>
<tr>
<td>F3</td>
<td>21st May 2009</td>
</tr>
<tr>
<td>F4</td>
<td>22nd May 2009</td>
</tr>
<tr>
<td>F5</td>
<td>11th June 2009</td>
</tr>
<tr>
<td>F6</td>
<td>12th June 2009</td>
</tr>
<tr>
<td>F7</td>
<td>18th June 2009</td>
</tr>
<tr>
<td>Mock</td>
<td>2nd July 2009</td>
</tr>
<tr>
<td>FTutorial</td>
<td>9th July 2009</td>
</tr>
<tr>
<td>Exam</td>
<td>17th July 2009</td>
</tr>
</tbody>
</table>

## DATES OF INTENSIVE FOI COURSES IN LONDON LEADING TO ISEB QUALIFICATION IN FOI

<table>
<thead>
<tr>
<th>CODE</th>
<th>DATES</th>
</tr>
</thead>
<tbody>
<tr>
<td>FN1</td>
<td>16th March 2009</td>
</tr>
<tr>
<td>FN2</td>
<td>17th March 2009</td>
</tr>
<tr>
<td>FN3</td>
<td>18th March 2009</td>
</tr>
<tr>
<td>FN4</td>
<td>19th March 2009</td>
</tr>
<tr>
<td>FN5</td>
<td>20th March 2009</td>
</tr>
<tr>
<td>Mock</td>
<td>27th March 2009 (tbc)</td>
</tr>
<tr>
<td>FTutorial</td>
<td>2nd April 2009</td>
</tr>
<tr>
<td>Exam</td>
<td>24th April 2009</td>
</tr>
</tbody>
</table>

## DATES OF DATA PROTECTION COURSES IN LONDON, MANCHESTER AND LEEDS LEADING TO ISEB QUALIFICATION IN DP

<table>
<thead>
<tr>
<th>CODE</th>
<th>MANCHESTER DATES</th>
<th>LEEDS DATES</th>
</tr>
</thead>
<tbody>
<tr>
<td>DN1</td>
<td>2nd March 2009</td>
<td>22nd June 2009</td>
</tr>
<tr>
<td>DN2</td>
<td>3rd March 2009</td>
<td>23rd June 2009</td>
</tr>
<tr>
<td>DN3</td>
<td>4th March 2009</td>
<td>24th June 2009</td>
</tr>
<tr>
<td>DN4</td>
<td>5th March 2009</td>
<td>25th June 2009</td>
</tr>
<tr>
<td>DN5</td>
<td>6th March 2009</td>
<td>26th June 2009</td>
</tr>
<tr>
<td>Mock</td>
<td>25th March 2009</td>
<td>3rd July 2009 (tbc)</td>
</tr>
<tr>
<td>DTutorial</td>
<td>1st April 2009</td>
<td></td>
</tr>
<tr>
<td>Exam</td>
<td>24th April 2009</td>
<td>17th July 2009</td>
</tr>
</tbody>
</table>

## Contributors

We would like to thank the following for their contributions to this edition:

- Kellie Blyth
- James Dimmick
- Candice Donnelly
- Yoram Hacohen
- Gemma Irving
- Richard Ives
- Ayesh James
- Rosemary Jay
- William Malcolm
- Karen McCullagh
- Joe McMorrow
- Fay Mitchelson
- Leonie Power
- Debbie Rees
- Imran Sadiq
- Vicki Southern
- Omer Tene
- Louise Townsend
Accountability for data security rests at the top, says Information Commissioner

In this edition, we devote the SOAPBOX column to the speech by Richard Thomas, the Information Commissioner, to RSA Conference Europe on data breaches, made on 29 October 2008. In his speech, Mr Thomas highlighted the risks associated with large databases, the need for tougher sanctions to deter data breaches and called on chief executives to take responsibility for the personal information their organisations hold. Arguing that information can be a toxic liability, he challenged CEOs to ensure that the amount of data held is minimised and that robust governance arrangements are in place. The Commissioner stressed that accountability rests at the top. CEOs must make sure that their organisations have the right policies and procedures in place, that privacy by design features are incorporated in the technology their organisations use and that staff are properly trained to counter the risks.

The year of “data insecurity”

The Information Commissioner began his speech by reflecting on the year of 2008, the year of “data insecurity”, a year which “has undoubtedly been the year of data breaches and data losses.”

He said “Data losses did not start with the loss of 25 million child benefit records by HMRC nearly a year ago. We had been warning of the problems for some time before then, but that was the case that undoubtedly catapulted the issue close to the top of the public and political agenda. Since then many other cases have hit the headlines. I can reveal today that the number of data breaches reported to my office has soared to 277 since November 2007. There have been 28 breaches by central government; 75 within the NHS and other health bodies; with 80 reported in the private sector. We are currently investigating 30 of the most serious cases. We have already taken enforcement action against HMRC, the Ministry of Defence, the Department of Health, the Foreign and Commonwealth Office, Virgin Media Ltd, Skipton Financial Services, Carphone Warehouse, Talk Talk, and Orange Personal Communications Services Ltd.

“The number of breaches brought to our attention is serious and worrying. I recognise that some breaches are being discovered because of improved checks and audits as a welcome result of taking data security more seriously. But the number notified to us must still be well short of the total. How many PCs and laptops are junked with live data? How many staff do not tell their managers when they have lost a memory stick, laptop or disc? How many organisations decide not to tell us? Many losses are simply undetected. Much more worrying is where – in an age of ever increasing cyber-crime, illegal access and identity theft – organisations are not even aware that personal information which they hold has been stolen, obtained by fraud or otherwise fallen into the wrong hands. Worse still, there are still organisations which are not aware of the risks that they face with any collection of data and have not taken adequate steps to deal with those risks. Worst of all, are those organisations who have simply failed to understand just how much personal information they are accumulating through more and more and ever-cheaper technology. Much is said and written about information being a valuable asset. It is also a toxic liability.”

The new information era

The Commissioner proceeded to say “Personal information is now the lifeblood of government and business and is central to our work, family and leisure time. The reality of the 21st Century is ever-increasing flows of digital data, revealing and recording almost everything we do, every transaction we undertake, our preferences and sometimes even our innermost hopes, worries and fears. Used properly and intelligently, personal information leads to better customer service, improved efficiency, more effective law enforcement and protection of the vulnerable and a better quality of life for everyone.

“But this means that respecting and protecting people’s privacy and personal information – data protection – has never been more important. As government, public, private and third sectors harness new technology to collect vast amounts of personal information, the risks of information being abused increases. It is time for the penny to drop. The more databases that are set up and the more information exchanged from one placed to another, the greater the risk of things going wrong. The more you centralise data collection,
the greater the risk of multiple records going missing or wrong decisions about real people being made. The more you lose the trust and confidence of customers and the public, the more your prosperity and standing will suffer. Put simply, holding huge collections of personal data brings significant risks."

**Sometimes lives may be at risk**

He added "It is therefore alarming that – despite high profile data losses, the threat of enforcement action, a plethora of reports on data handling and clear Information Commissioner Office guidance – the flow of data breaches and sloppy information handling continues. Of course it is important to recognise that incidents vary from regrettable one-off and probably unavoidable accidents to wholesale and systematic failure to take information security seriously. But everyone must also recognise that data breaches can cause harm, distress and hassle for the individuals affected, can lead to serious financial losses and can seriously affect the reputation of organisations.

We have already seen examples where data loss or abuse (sometimes linked to identity theft) has led to fake credit card transactions, witnesses at risk of physical harm or intimidation, offenders at risk from vigilantes, fake applications for tax credits, falsified Land Registry records and mortgage fraud and exposure of the addresses of service personnel, police and prison officers and battered women. Sometime lives may be at risk. There have already been cases for example where prison staff have had to be relocated because of security concerns.

"There must be a wake-up call each time there are headlines about unencrypted laptops which have gone missing, health or financial records found in the streets or memory sticks or hard drives which cannot be accounted for. But are there still too many people asleep at the helm?

"This is a central challenge for those who lead all private and public organisations. The custodians of our data must earn and retain our trust and confidence. They have the responsibility to ensure that it is kept safely and in line with the requirements of the Data Protection Act. This is not just a matter of security. It will never be possible to eliminate losses and data breaches entirely. This simply emphasises the importance of data minimisation; collect, use and store no more personal information than is necessary and keep it for no longer than necessary."

**The way forward**

Mr Thomas said "All of this must ultimately be a matter of good governance and accountability. There is no single magic bullet, but there will always be three key elements:

- Clear thinking and paperwork – ensuring the right policies, procedures, contracts, compliance arrangements etc.
- Getting the technology right – awareness of the power of technology, the risks of ever-cheaper storage and mobile data and looking to use technology to minimise risks – "Privacy by Design".
- Focusing on people and behaviour – recognising that the challenge is cultural and psychological – and must be led from the top – with the right approaches to awareness programmes training, managements, and supervision.

"Those at the top of organisations – chief executives, permanent secretaries and so on – must be certain that the right framework is in place to address the risks of personal information and must be certain that responsibilities are clear. There must be complete clarity on who, inside each organisation, has responsibility for safeguarding each set of personal data. This is equally important where data is shared, sometimes amongst several sources, and where processing is outsourced to contractors. Given the levels of risk, there is also a role here – as we elaborated in the Thomas/Waipoort Report on Data Sharing – for reinsurance to be provided through Audit Committees and Statements of Internal Control in annual reports. This should be enlightened self-interest and bodies such as the CBI can help to ensure adequate controls and disclosures. But the Financial Reporting Council and others will need to intervene if high-level accountability is not achieved in practice.

"There is also an important role for my Office as the regulatory body, with a role to educate, scrutinise and police. As approaches to regulation become less light-touch, the law plays an increasingly important symbolic and substantive role in showing that data protection must be taken seriously. I have already mentioned that we have taken enforcement action in suitable cases, but the current law has limited impact. We (and many others) have long argued that our powers, sanctions and resources – fixed in another era – are now wholly inadequate. The Information Commissioner’s Office (ICO) has made clear for some time that a stronger approach is required to help prevent unacceptable information handling. At last there is movement. Earlier this year Parliament decided that the ICO should have the power to impose substantial penalties for deliberate or reckless breaches. I understand that the government is working to ensure this measure is implemented as soon as possible. The threat and reality of substantial penalties will concentrate minds and act as a real deterrent. The notification fee for the largest organisations needs to be increased to give the ICO the resources we need to do our job properly. We are also looking forward to new powers to undertake inspections and audits of data controllers."

**A word of warning about breach notification**

In respect of the much discussed subject of breach notification he said "It is unfortunate that it has taken calamity to convince the government that we need stronger powers, resources and sanctions, but we must also take care not to overreact. We do not need laws for their own sake or ill-considered laws. I am very sceptical about the value or viability of laws requiring individuals to be notified when there is a breach. When personal information has been lost, stolen or otherwise compromised, the immediate priority is to manage the security breach and take all necessary steps to reduce the risks to individuals and to the integrity of the organisation’s operations.

"As a matter of good practice, the ICO should be contacted immediately when any significant breach is discovered and, with the benefit of risk assessments applying to the particular situation, we can ensure that individuals who are affected are being told where that is necessary or genuinely useful.

"But I do not favour placing a statutory duty on organisations to notify people directly whenever a breach occurs and I am doubtful that a satisfactory law could satisfactorily distinguish in advance between situations where notification is needed and those where it is not. Each breach carries different levels of risk and, consequently, requires a different response. Unless written and interpreted with very great care, a mandatory notification requirement would add a significant extra burden for organisations and, more worryingly, could produce 'breach fatigue' if it were to result in frequent and unnecessary notifications of minor incidents. This carries the very real danger that people will ultimately ignore notifications when there is, in fact, significant risk of harm. Notifying people, when there is often not much they can do about the situation wrongly shifts responsibility from the organisation to the individual and diverts attention and resources away from prevention. Put simply, where the risks posed by security breaches are serious, a notification requirement would be too timid. If they are not, it would be excessive."

**The Information Commissioner**

**Richard Thomas**