IBM tops workplace privacy poll

A study carried out by US-based *Wired Magazine* has claimed that IBM is one of the top companies when it comes to respecting workers' privacy. The technology company has been applauded for its pro-privacy practices which date back to the 1960's. One initiative carried out by IBM includes requiring its healthcare partners to erase employees' social security numbers from its records. Other companies acknowledged for good privacy practice included Hewlett-Packard, Ford, and Baxter Healthcare.

According to the study, the worst performer was pharmaceutical company Eli Lilly which, claims *Wired Magazine,* "freaked after 9/11" by carrying out background checks on contract workers and dismissing some for minor offences. Also reported to have poor staff privacy procedures were the Wal-Mart and Hilton Hotels chains.

Sonera telecoms scandal widens

Finland's National Bureau of Investigation (NBI) suspects that telecoms operator, Sonera, may have breached the privacy rights of thousands of individuals during 2000/2001. According to Finnish newspaper, *Helsingin Sanomat*, the NBI believes that Sonera illegally traced the telephone calls and e-mails of around 7,000 people, including staff, members of the Sonera board, and journalists.

In October last year, *Helsingin Sanomat* alleged that the company had tracked the communications of people suspected of leaking negative comments about the financially troubled company. Following the report, police arrested senior corporate security staff, as well as former chief executive, Kaj-Erik Relander. The initial investigation focussed on the suspected surveillance of around 100 employees of the telecoms operator, but the NBI now believes that thousands of others may have been caught up in the operation. A maximum prison sentence of up to three years could be imposed on anyone found guilty of conducting the alleged surveillance.

The NBI has recommended that prosecutors limit their scope to the initial 100 suspected privacy violations in order to reduce the administrative burden on the state. But *Helsingin Sanomat* has pointed out that any other concerned individuals could initiate their own privacy action.

According to *Reuters*, Jyrki Karasvirta, Sonera's vice president of Brand Marketing and Communications, said it would be difficult to gauge what impact these events will have on the company, which was taken over at the end of last year by Swedish operator Telia to form a leading player in the Nordic region. "Of course, it is not doing good for the image of the company," he said. "But one must remember we are discussing an incident which might have taken place a couple of years ago."

See PL&B International, Feb 2003, p. 5 for previous coverage.

South African websites poor on privacy

A study of the top 100 South African websites carried out by the University of Cape Town has identified a spate of poor privacy practices. According to *Business Day*, 96 of the sites studied collect personal data, yet only ten provided sufficient notice about how that information would be used.

More worryingly, over 90 per cent of the sites collecting personal data share it with third parties without obtaining individuals' consent. Only 24 sites provided an opt-out facility for marketing preferences, while 5 provided an opt-in. A quarter of the websites allowed consumers access to their data.

Worst performers were government-run websites, while the most compliant came from the retail sector.

France provides opt-out for telecoms directories

On August 1st, the French government passed a decree allowing consumers to prevent their details from being included in a publicly available telecoms directory. The decree permits the creation of a "universal directory" gathering together the details of all telephone users, including 38 million French mobile phone subscribers.

In order to protect consumers' privacy rights, France's data protection authority (CNIL) recommended that individuals be allowed to sign up to a free "red list" which will prevent personal data from being listed in the directory. A second "orange list" will allow customers to be listed in the directory, but prevent certain information, such as their address or first name, from being listed. In addition, those registered on the orange list will have the right to prevent marketing communications being sent to them and stop the use of so-called reverse searching (eg. searching for people via their telephone numbers).

Communications service providers must provide customers with information as to how their details will be used and give them six months to register their preferences, after which they will be included in the directory, although their details will not be used for direct marketing.

In addition to the list, the decree allows the CNIL to tackle the problem of unsolicited marketing via fax and automated calling systems by imposing a €750 fine for each message sent.

For further information, see:
www.cnil.fr/actu/frame.htm?http://www.cnil.fr/actu/communic/actu54.htm

Canadian Privacy Commissioner resigns under a cloud

George Radwanski, Canada's federal privacy commissioner, resigned in June only days before the release of a House of Commons committee report that repeatedly stated its loss of confidence in the commissioner. "We believe the Commissioner has deliberately misled the Committee on several recent occasions, and we have therefore ceased to be confident in the completeness and accuracy of information communicated by the privacy commissioner to Parliament, and the Committee.

Although the focus of the committee's report was Radwanski's deliberate misleading of the committee, it found further significant fault with his conduct and called on Canada's Auditor General and the federal Public Service Commission to investigate, respectively, his financial affairs and hiring practices:

"[T]estimony we have received during the past several weeks has also left us, in addition, with growing concerns about the financial and administrative practices of the Commissioner, and his Office...More broadly, testimony received from several employees relating to a personal style that appears to rely heavily on intimidation and bullying has deepened these concerns...In short, as a consequence of the evidence accumulated by the Committee, we came to lack confidence in the Privacy Commissioner and his capacity to perform his duties to Parliament and the people of Canada."

The former commissioner also encountered a staff revolt, when many members of his staff signed a petition calling for him to step down and then participated in a temporary walkout.

Radwanski resigned four days before the committee report was released. However, the committee reported that, had he not resigned, it would have recommended that the House of Commons and Senate adopt a motion to remove him from office - an action without precedent in Canadian parliamentary history.

The day before the committee report's release, the government appointed an interim privacy commissioner, Robert Marleau, a respected former clerk of the House of Commons. Marleau will hold the position until January 2004, at which time an as-of-yet unnamed privacy commissioner will assume the post. In addition, on August 13th, the government announced the appointment of two deputy privacy commissioners - Heather Black, general counsel with the Office of the Privacy Commissioner, and Raymond D'Aoust, of the Canadian Centre for Management Development. Black in particular has a long association with privacy issues, including her extensive work on the development of Canada's federal private sector data protection legislation, the Personal Information Protection and Electronic Documents Act.

Report by Eugene Oscapella

California enacts data security law

On July 1st, a new US state security law (California SB 1386) came into force that will require US businesses holding data on Californian residents to notify them of any security breaches which result in the theft of personal data. The law was enacted in an attempt to combat the increasingly common threat of identity theft, with the intention of making individuals more aware of any unauthorised access to information such as credit card details, car licence plate numbers, telephone numbers, and credit information. Figures from the Federal Trade Commission claim that 27.3 million Americans have been victims of identity theft over the last five years.

The law states that businesses should "disclose any breach of the security of the system...without unreasonable delay." However, there is a noticeable exemption to the new law. Companies that encrypt their customers' details do not have to disclose any security incidents that occur.

Despite a flurry of media reports over the last few months, businesses and their staff remain unaware of the new law. According to a survey conducted by Harris Interactive, on behalf of security firm, Vontu, only 6 per cent of the 500 employees questioned had heard of SB 1386. "There is considerable lack of awareness of this new law among the workers who will be most impacted by its sweeping implications," said Joseph Ansanelli, CEO of Vontu. "The results of this survey indicate the state of California may need to do more to notify companies of this new law."

US security and privacy expert Robert Smith said that the notification requirement will prove problematic for businesses. Speaking to *Reuters* he said: "Once you have a break-in, you really don't know what's been taken. This is going to be a big burden for companies to have to send out these notices."

In many cases, business will have to provide written notices to their customers. However, restrictions on the type of notice businesses are required to give will be relaxed under certain conditions. If the cost of providing a notice exceeds $250,000, or the number of customers affected by a breach exceeds 500,000, then businesses can provide notice via e-mail, a posting on the company website, or a warning through state press or broadcasters.

Online privacy confuses US web surfers

According to research by the Annenberg Public Policy Center, American Internet users just do not understand how online business practices are affecting their privacy. A survey of 1,200 people showed that less than half could understand website privacy policies. Of those that did, 57 per cent incorrectly believed that by posting a privacy policy a company was automatically stating that it would not share customer details with other companies.

The survey also revealed a poor understanding of the various ways in which businesses track and collect personal data, match it up with other pieces of information, analyse it and then use it for a multitude of purposes. "Even if people have a sense that sites track them and collect individual bits of information, they simply don't fathom how those bits can be used," said Joesph Turow, Professor of Communications at Annenberg.

However, despite the confusion, individuals are worried about how their personal data will be used. When presented with details on how companies can exploit their information, 85 per cent indicated that they would not accept such practices.

But although there were strong objections, the survey revealed that few people actually take steps to prevent the misuse of their details. 64 per cent indicated they had taken no action whatsoever to protect their privacy, while only 9 per cent said they knew how to prevent their details from being misused.

The complexity of technology and its impact on privacy indicates why an overwhelming majority of the individuals questioned support legislative solutions rather than reliance on industry goodwill. 95 per cent wanted to have a right of access to any information a company holds on them, while 84 per cent believed that a law giving them control over the use of their personal data would be an effective solution to the problem.

"At a time when technologies to extract and manipulate consumer information are becoming ever-more complex," said Turow, "citizens' ability to control their personal information must be both more straightforward and yet more wide-ranging than previously contemplated."

He proposes three recommendations. Firstly, federal legislation should be introduced to require all online businesses to build the P3P (Platform for Privacy Preferences) privacy standard into their websites. He claims that by mandating P3P, the ambiguities as to how and with whom information is shared will be reduced.

Secondly, Turow suggests that organisations should be required to disclose their data flows to customers, explaining what information is collected, if the data will be linked to other information, whether it is shared with third parties, and what the information will be used for.

Thirdly, he proposes the introduction of privacy audits (with the costs borne by businesses) to ascertain whether an organisation is P3P-compliant and its data handling practices match its privacy policy. Any discrepancies could then be pursued under the Federal Trade Commission's deceptive practices rules.

For a copy of the research, 'Americans and online privacy: The system is broken', see www.appcpenn.org.

EU regulators call for biometrics privacy code

The EU Article 29 Data Protection Working Party (a group of European data protection authorities) has recommended the creation of a code of conduct governing the use of biometric technologies (eg. fingerprint, iris, or voice recognition systems) to identify individuals.

Organisations are increasingly turning to biometric solutions as a means to improve security and access controls, monitor the comings and goings of employees, and reduce the risks of identity theft.

But, in a paper published at the end of August, the Working Party voiced a number of privacy concerns and called for the IT industry to enter into dialogue with data protection authorities to discuss ways of developing biometric solutions in a "data protection-friendly manner".

One major concern is that by storing biometric data onto central databases, individuals' personal data could be used for wider purposes than originally intended. To reduce the potential privacy risks, the Working Party states that "biometrics should preferably not be stored in a database but rather only in an object exclusively available to the user, like a microchip card, a mobile phone, [or] a bank card."

The report makes a number of other recommendations for the use of biometric technologies. These include providing individuals with information on how their data will be used, destroying any unnecessary data that is collected, putting proper security measures in place and, in certain circumstances, receiving prior approval from data protection authorities before implementing new systems.

Despite concerns, the Working Party recognises the validity of biometrics, stressing that they could be used as privacy enhancing technologies (PETs) - for example, by reducing the need to collect additional personal data, such as individuals' names or addresses.

For the full text of the Working Party's opinion, see: http://europa.eu.int/comm/internal_market/privacy/workingroup/wp2003/wpdocs03_en.htm

Privacy and Human Rights report published

The Electronic Privacy Information Center and Privacy International have published a new report on 'Privacy and Human Rights' for 2003. The report provides an update on data protection developments such as government and private sector surveillance, public sector privacy, workplace monitoring, technology advances and genetics. The report also provides a detailed update on the legislative developments in over 55 countries.

Privacy and Human Rights 2003 has highlighted a number of threats to privacy and civil liberties following the September 11th terrorist attacks in 2001. Concerns have been raised over data sharing between law enforcement agencies, 'function creep' in anti-terrorism laws and the increasing use of technology to track and profile individuals. There has also been major developments in the use of national ID cards, video surveillance, and biometric identification systems.

Despite some negative conclusions, the report also notes positive changes over the last year, including data protection developments in Eastern Europe, and the introduction of new privacy laws in Luxembourg, Ireland and Malta.

For a copy of the report: www.privacyinternational.org/survey/phr2003

PGP Corporation launches business-friendly encryption tool

In September, encryption specialists, PGP Corporation, released a new secure messaging tool to help businesses comply with security and privacy regulations. The PGP Universal 1.0 product suite has been designed to provide businesses with a simpler, more manageable means of encrypting confidential communications.

The PGP (Pretty Good Privacy) encryption standard has experienced ups and downs since its creation in the early 90's. After being bought by Network Associates Inc (NAI) in 1997, high hopes for commercial success were dashed when, five years later, NAI dumped PGP after failing to exploit its potential.

But the premise of secure messaging remains a valid one. With so much confidential data being exchanged, there is a growing need to implement strong security controls. Lawyers need to protect client confidentiality, CEOs want to be sure that business plans will not be exposed, while legislation such as the EU Data Protection Directive and the US Health Insurance Portability and Accountability Act (HIPAA), has made the protection of personal data a legal requirement.

However, widespread adoption of encryption tools has been slow as they have not traditionally been very user-friendly. Organisations have either avoided it altogether or rolled it out to a select few 'critical users' only.

But now the PGP Corporation, which bought the rights to PGP last year, has developed a more functional and corporate-friendly version of the encryption tool. By taking the whole process away from users' desktops and putting it onto the corporate network, PGP Universal provides a more cost-effective means of providing secure messaging across the enterprise.

Taking the functionality out of users' hands makes it simpler for staff to send secure e-mail, and allows organisations to enforce their security policies by automatically determining which messages should be encrypted. While previously, users would have to remember to encrypt confidential material, now they have no choice but follow the corporate policy.

Additionally, PGP Universal will allow businesses to enforce their security standards on partners or vendors by ensuring that any replies to secure communications are also encrypted.

PGP Corporation also believes it has solved the problem of sending secure mail to external contacts that do not have similar encryption software. The new system allows third parties to access PGP-encrypted mail through a password-protected web mail system, or by downloading encryption keys via a 'satellite' system.

For further information: www.pgp.com

US facial recognition system branded a failure

A Virginia newspaper reports that a facial recognition system in place for about a year in the city of Virginia Beach has failed to catch a single wanted person. City police argue, however, that this is because no one in its database of "mug shots" walked into the line of sight of any of the three cameras that used the technology. The system has room for 30,000 mug shots to be matched against video images of people walking along the city's ocean front.

This result would be no surprise for critics of the technology. The American Civil Liberties Union (ACLU) obtained 2002 documents on the facial recognition system installed at Palm Beach Airport in Florida. The system failed to match volunteer employees who had been entered into the database 503 out of 958 times, or 53 percent of the time. "Even with recent, high quality photographs and subjects who were not trying to fool the system, the face-recognition technology was less accurate than a coin toss," said Barry Steinhardt, director of the ACLU's Technology and Liberty Programme. "Under real world conditions, Osama Bin Laden himself could easily evade a face-recognition system."

Report by Eugene Oscapella

News in brief

WORKPLACE PRIVACY

According to law firm Baker & McKenzie, the Norwegian Data Inspectorate has informed transport company, SVIPP Transport, that it can no longer require job applicants to provide sensitive details on their medical and criminal backgrounds. The Inspectorate ruled that SVIPP did not have a justifiable reason for requesting the information.

On June 26th, the Finnish government published a draft law to replace the existing Data Protection in Working Life Act which came into force in 2001. The government's proposals will allow businesses greater scope to monitor their employees' communications, conduct CCTV surveillance, and carry out drug testing.

Workers at Qantas have threatened strike action over the Australian air carrier's plans to introduce random drug testing on its staff. According to news service *AAP*, employees would also be required to provide managers with details of any prescription medication, such as heart disease and psychiatric drugs, or Viagra.

A spokesperson for Qantas said the testing is necessary for health and safety purposes, but added that staff privacy would be respected. See p.16 for more on drug/alcohol testing in the workplace.

According to the *Associated Press*, an employee of the US Federal Bureau of Investigation has filed a privacy lawsuit alleging that his employers disclosed details of his personnel file in efforts to discredit him.

Robert Wright, who works in the Chicago branch of the FBI's anti-terrorism unit, had criticised the agency's anti-terrorism efforts prior to the September 11th attacks in the US. Wright now alleges that the FBI has attempted to discredit him by informing reporters that he was the subject of two internal affairs investigations.

EU companies challenged by workplace monitoring rules

Organisations that operate across multiple EU jurisdictions face a bewildering set of obstacles when planning to monitor workers' use of corporate communications systems such as e-mail and the Internet.

A report published in September by the European Industrial Relations Observatory (EIRO) looked into how communications monitoring is handled across Europe. Its findings show that businesses carrying out employee monitoring are having to deal with a complex range of regulatory requirements, including constitutional provisions on privacy, employment law and labour codes, technology-related privacy laws, and mediation with national works councils.

The report notes that EU member states have "several kinds of legislation relating to the protection of privacy". It states that "it is rare for countries to have introduced specific legislation applying data protection rules to the employment context." The most notable exception is Finland which introduced its Act on Data Protection in Working Life in 2001. The Finnish government now has plans to replace the Act with a more business-friendly law.

Many member states include general privacy provisions in their national constitutions that can be applied to the workplace. Additionally, employment law can also contain provisions on workers' privacy. For example, the report says that the "French Labour Code prohibits restrictions of workers' rights and freedoms except where justified and proportionate." (see *PL&B Int*, May/June, p.30) Portugal's new Labour Code also has provisions on workers' right to privacy.

Other EU countries have created technology-related laws that can be applied to the workplace. For example, in 1982 Denmark passed the Act on Video Surveillance, while the UK has implemented the Lawful Business Practice Regulations which set out requirements on the interception of communications by employers.

Works councils also have input into the use of monitoring in the workplace. In Austria, Germany, Luxembourg and the Netherlands, co-determination is required before introducing monitoring technologies. And in Belgium, Finland and Spain, employers are required to consult with their works councils.

The lack of specific legislation on workplace privacy, says the report, places a greater emphasis on case law to determine the correct approach to employee monitoring. Court rulings in these cases vary from country to country, and even "judgments from the same country may appear contradictory," says the report. However, there are common themes running through cases involving e-mail and Internet use. In Denmark, Germany, the Netherlands, and the UK, cases "have established the necessity for employers to have issued a clear policy or instructions on Internet/e-mail use before it is legitimate for them to dismiss or discipline employees on grounds of misuse."

Courts are more likely to rule in favour of employers in cases which involve the use of communications to access pornographic, discriminatory or violent material, and to commit acts of harassment or defamation.

The European Commission is currently looking into the pros and cons of a workplace privacy directive in an attempt to combat the lack of harmony between various member states' approach to the issue. Although the Commission is expected to propose a directive in 2004 or 2005, its plans have met with opposition from employers' representatives. The Union of National Industrial and Employers' Confederation of Europe (UNICE) has hit out at the Commission, stressing that the existing EU Data Protection Directive already provides sufficient protection and that further regulation would be a burden on the business community.

EIRO's report can be found at: www.eiro.eurofound.eu.int/2003/07/study/TN0307101S.html