Debate over DP laws follows Deutsche Telekom scandal

An argument is already raging over the efficacy of privacy legislation even though the scope of the phone-monitoring affair is unclear. By Dugie Standeford.

Since allegations surfaced in May that Deutsche Telekom illegally monitored telephone call records in an effort to stop damaging leaks by board members to journalists, scarcely a day has gone by without new developments. Things are far from resolved, with ongoing investigations by German prosecutors, the telecommunications regulator, the federal privacy chief and the company itself.

Deutsche Telekom issued its first statement on the situation on 24 May. It acknowledged findings of “misuse of call records” – not tapping of content but monitoring of call times, durations and participants – in 2005 and 2006. The company was tipped off about a similar individual case in the summer of 2007 and was able to

Turkey applies to DP club; DP part of EU application

The government of Turkey sent to parliament a bill to protect personal data on 24 April 2008. It is now pending before the Justice Committee. This adds to a bill introduced two weeks before on transparency and state secrecy. Both bills are part of the country’s campaign to become a member of the EU. The two bills would establish two independent councils to supervise their implementation. The privacy law would define personal data and set out circumstances in which the state may collect personal data, and when such personal data may be transferred to third parties. It also would impose criminal penalties.

No agency will have authority to register information about an individual’s race, political opinions, philosophical beliefs, religion, denomination or other type of convictions, membership in an association, foundation or a union; health condition; or private affairs. The bill also would impose restrictions on police records. It would allow collection of personal data only in cases where such collection would not be a breach of private or family life and where the public interest requires such collection, and only so long as there is legislation ensuring the confidentiality of such data. The bill would establish citizens’ right to know whether personal data about them has been recorded; the right to review any such data; and the right to correction in cases of erroneous, mistaken or inadequate data.

The bill introduces jail sentences

Continued on p.3

Continued on p.3
No end of a privacy lesson, and no end to learning

In 2002, Hewlett-Packard created the Privacy Innovation Award and in 2005 was joined by the International Association of Privacy Professionals (IAPP) in sponsoring it. Then in 2006 came the HP boardroom leak inquiry which has cost HP millions of dollars, several very high officers their jobs, and is still having unpleasant consequences (p.4). At the end of 2007, Privacy International named Greece as one of the most privacy protective countries in the world. Before a year had passed, nearly all members of the Greek data protection authority resigned in protest at being overruled by the government over the use of closed-circuit television cameras. Deutsche Telekom has an admirable programme of data protection (pp.21-23), but someone in the group clearly was not reached by it (p.1). They probably will not be the last to believe that privacy and data protection principles had been safely taken on board, only to find to their embarrassment that some of the principles had slipped off for what someone thought was a good reason at the time to make some exceptions.

Data protection is about more than the latest round of national legislation (Turkey, p.1), enforcement actions (France, p.5, Italy, p.16, Hong Kong, p.13) and judicial rulings (Germany, p.9) which are merely of concern to the compliance department. It is about a corporate culture that sees respect for privacy as a positive value in attracting customers and which incorporates privacy from the shopfloor or officefloor to the boardroom. In times of economic stringency it is tempting to regard data protection as a non-vital area for expenditure, with compliance kept to the legal minimum. To do so would be to ignore the carrot of public and consumer confidence when those are becoming scarce, and to risk slips that could come in for some very expensive stick.

James Michael, Editor

Contribute to PL&B newsletters

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact James Michael on Tel: +44 (0)20 8868 9200 or e-mail james.michael@privacylaws.com.
wrongfully disclosed on its website personal and sensitive business data, including passport details, related to trademark registration.

Other countries have faced their own data breach controversies. Last year, Japan’s National Police Agency banned its officers from installing file-sharing software on their private computers and from taking home investigation files after similar data leaks made it onto the Internet. In the UK last November, the British government reported its biggest data breach to date, the loss of computer disks containing detailed personal information – such as bank account and national insurance numbers – on 25 million Britons, or 40% of its population, prompting a public apology by the Prime Minister to the nation. And the incidents of publicly reported data breaches in the U.S. rose by more than 40% in 2007, according to a study by Identity Theft Resource Center, a consumer rights advocacy group.

LOOKING AHEAD

Woo and others say that Hong Kong – once a leader in private data protection, as one of the first jurisdictions outside Europe to have a data protection law – now needs to review and update its 12-year-old law to take into account new technologies and new realities. Woo points to the efforts of Canada, New Zealand and Australia, which have begun reviewing their data ordinances in the past several years.

The Privacy Commission reviewed the Personal Data (Privacy) Ordinance in 2006, according to Woo, and submitted a proposal to the government with more than 50 recommendations, including a call for a public consultation and amendments to enhance the ordinance’s effectiveness. Changes being considered include a requirement of official notification of all data breaches to the Privacy Commission and a new definition of personal data.

Also on Woo’s wish list is more funding. The commission is given HK$37 million annually for operational costs and will receive an additional HK$2.8 million for 2008-2009 to hire more staff and promote public awareness of privacy issues. But Woo has urged even more resources in light of the latest revelations. His office, he says, might not be able to continue to inspect personal data systems – invoked for the first time in May at public hospitals – if increased funds are not forthcoming.

Other agencies are also conducting investigations. The Hospital Authority has appointed a four-member task force, which includes Charles Mok, chairman of the Hong Kong Internet Society, and Stephen Lau Ka-men, former privacy commissioner. A police working group led by the deputy commissioner for operations is examining the police incidents and overseeing a comprehensive review of police guidelines on Internet security, including how officers can use their personal computers at home.

In a statement to the Legislative Council, the Hong Kong government acknowledged the “public concern” over the incidents, particularly noting that “popular use of and reliance on the Internet as a platform for doing business, work, study, leisure, etc. also creates online threats.”

It has vowed to improve staff awareness of information-security requirements in order to ensure compliance and minimise the occasions on which data is stored on portable devices.

Cyber fury and law revision in Korea

Lawsuits urged for data breaches, DP law revised, presidential impeachment Internet postings blocked. By Whon-il Park.

May is the month for South Korean families to observe Children’s Day and Parents’ Day. It is also a time when young Korean students and citizens are expressing their views and opinions on the Internet and are taking to the streets in peaceful candle-lit processions.

DATA SPILLS AND QUASI-CLASS ACTIONS

The first issue was a large scale leakage of personal data from the largest online market place, Auction, an e-Bay subsidiary in South Korea. Eleven million customers, one quarter of the population of Korea, were affected by the incident, caused by an unidentified third-country hacker. Soon after this incident, one of the biggest common carriers in Korea, Hanaro Telecom, was allegedly providing personal data of its customers to telemarketers without consent of the data subjects.

Although American-type class actions are not allowed for the users of telecommunications services in Korea, several aggressive lawyers are advocating via Internet sites that customers mentally or financially affected by these incidents bring lawsuits against Auction and Hanaro Telecom. Recently, this kind of lawsuit has been somewhat productive in terms of damages, from $100 to $700 per plaintiff.

However, experts are warning that this kind of conventional lawsuit initiated by some interested plaintiffs could not compensate all the affected users and might enrich only lawyers, and eventually undermine the ISP business itself. So they are urging the legislative adoption of the US-type class actions, currently allowed only in securities fraud cases.

LATE REVISIONS TO DP LAW

On 22 May 2008, in the final days of the current National Assembly, the...
Italian online tax posting unlawful

Outgoing government’s Parthian shot condemned. Amy Norcup reports from Rome on why the Italian Ministry of Finance acted unlawfully in publishing Italian residents’ tax returns online.

On the evening of 29 April the Italian tax authority placed tax records for 38 million Italians on their website, detailing declared income and tax figures for 2005. Also listed were the names, addresses and the birth dates of all taxpayers. For accessibility, the tax authority had also tidily listed records alphabetically and in order of region. For the first time, without any reason, Italians could see their own records online as well as having access to their neighbour’s financial profile and the high earnings of the rich and famous. By Wednesday 30th April there was a “news crash” with media coverage prompting thousands of Italians, curious to learn what the rest of the country was earning, to log onto the website and access the data firsthand.

However, the mad dash caused the website to crash and was subsequently followed by two orders from the Garante per la Protezione Dei Dati Personali (Data Protection Commission), having learnt of the unprecedented posting of such data on the Internet:

1. An order to the tax authority to block the site
2. An order to the media not to “circulate the data further” unless it can be shown that it was in the “public interest” to do so.

Two days had lapsed before the head of the Garante, Professor Francesco Pizzetti, on 2 May could make such orders, as he requested, in a letter sent to the revenue office, seeking clarification of their actions before making any formal decision on the matter. Despite the tax authority replying, on time, and justifying their act on grounds of “transparency” for the purposes of tax evasion on 5 May, the Garante declared a day later on 6 May that the Italian Revenue Office, had in fact published the data unlawfully. The decision was published on the DPA’s website and the Garante requested, in their statement, that the tax authority were to publish their decision “to the widest possible extent” including publication in the Official Journal of the Italian Republic.

The Garante’s reasoning behind judging such an act unlawful was three-fold:
1. The publication of the lists via the Internet was in breach of Italian Data laws, with the Italian Ministry of Finance acting unlawfully in publishing Italian residents’ tax returns online.

Ongoing government’s Parthian shot condemned. Amy Norcup reports from Rome on why the Italian Ministry of Finance acted unlawfully in publishing Italian residents’ tax returns online.