Durant takes right of access case to the EU

John Durant, the man whose failed battle against the Financial Services Authority (FSA) has redefined the UK data protection landscape, has filed a complaint with the European Commission. And experts have warned that if the Commission decides to investigate, the UK government could be forced into amending the Data Protection Act (DPA).

In December last year, Durant lost a case in the Court of Appeal in which he tried to force the FSA into handing over documents relating to a dispute with Barclays bank. The documents were requested under section 7 (the right to access personal data) of the DPA, but the Court of Appeal refused him access to the disputed information, arguing that it did not constitute personal data and that the paper-based records requested fell outside the scope of the DPA.

Many data protection experts, however, have raised doubts over the Court of Appeal's ruling, arguing that the overly restrictive interpretation of the DPA could conflict with individuals' rights to access information about themselves. Speaking at the Advanced Legal Data Protection and Privacy Forum in London on May 19th, Kirsten Houghton, the Quadrant Chambers barrister who represented Durant in the Court of Appeal, criticised the court's decision, arguing that the ruling "has raised more questions that it has answered". She was especially critical on the issue of how much discretion courts have in forcing organisations to hand over requested information. "My personal view," said Houghton, "is that if the European Commission do take this [complaint] up, there's a very good chance that they will find that the Data Protection Act has been interpreted wrongly."

Houghton also criticised the legal accuracy of guidance published by the Information Commissioner in the wake of the Court of Appeal ruling. "The guidance is frankly not very good and needs some help," she said. The Information Commissioner, Richard Thomas, later defended the post-Durant guidance saying that "businesses have found it very helpful". But, he added that the Commissioner's office would be publishing a revised version of the guidance to clarify areas that have caused confusion.

See www.informationcommissioner.co.uk for more information.

News in brief

UNITED STATES - The Federal Trade Commission (FTC) is considering regulations that would force companies to offer consumers an opt-out choice over sharing their data with affiliate companies.

The proposed regulations would bring into force dormant provisions contained within the Fair and Accurate Credit Transactions (FACT) Act. The Act, which was introduced in December last year, provides consumers with greater access to their personal data, protection against ID theft and stronger privacy choices.

Comments regarding the proposed regulations can be sent to www.regulations.gov

AUSTRALIA - On June 17th, the Australian government passed the Electoral and Referendum Amendment Act, banning the use of the electoral register for commercial purposes such as direct marketing or debt collection.

FTC backs away from do-not-spam registry

A 'do-not-spam' registry is likely to cause more harm than good, according to the Federal Trade Commission (FTC) which advised the US Congress in June to shelve plans to introduce a national opt-out register for e-mail addresses.

Although the introduction last year of a similar registry targeting unwanted telemarketing calls has proved a remarkable success, the FTC believes that an anti-spam list will simply act as a source for spammers to harvest e-mail addresses.

Under the CAN-SPAM Act, which came into force at the beginning of this year, the FTC was tasked with investigating the feasibility of introducing a do-not-spam registry. But following consultation with consumer and marketing groups, ISPs and computer experts, it has concluded that until methods for identifying spammers improve, the privacy and security of such a registry would be placed at considerable risk.

In a report to Congress, the FTC said that "spammers would most likely use a regsitry as a mechanism for verifying the validity of e-mail addresses and, without authentication [of spam e-mails], the Commission would be largely powerless to identify those responsible for misusing the registry."

Instead, the FTC is proposing a programme to improve e-mail authentication standards that will allow ISPs to identify and track down spammers that try to conceal their identities.

In fact, the FTC considers that if industry can implement the right technology and regulators can effectively enforce the CAN-SPAM Act, the need for an opt-out registry may become obselete.

For a copy of the report: www.ftc.gov/reports/dneregistry/report.pdf

JetBlue and Acxiom named in privacy lawsuit

US air carrier JetBlue and information management solutions provider Acxiom have both been named in a federal privacy lawsuit according to *USA Today*. JetBlue was accused last year of violating privacy assurances after handing over the details of more than a million customers to a US defence department contractor, which has also been named in the lawsuit (*PL&B International*, Oct/Nov 2003, p.1). The contractor, Torch Concepts, used the data in a project aimed at finding ways of screening for terrorists. Acxiom handed over additional demographic data on JetBlue's customers, such as social security numbers, income, number of dependents etc.

Although JetBlue has since apologised over the violation of its privacy policy, Acxiom appears more reluctant to face up to the charges. David Kramer, the attorney representing Acxiom told *USA Today*: "Acxiom shouldn't be a party here, and we're going to try and convince the court of that as the case moves forward."

The likelihood of the lawsuit succeeding, however, was placed in doubt after a similar case against Northwest Airlines was thrown out by a US district court judge. Northwest were accused of infringing the privacy of its customers when it handed over their details to NASA in December 2001. The judge ruled that concerns over the security of the US transportation sector meant that the disclosure of customers' data was legitimate. The case was also dismissed partly because it could not be shown that the plaintiffs had actually read Northwest's privacy policy.

The National Business Travel Association (NBTA) has published a set of guidelines for airlines on the privacy issues around the disclosure of customer data to the US authorities. See www.nbta.org.

Access to corporate data cheaper than a McDonald's meal

Laptops and hard drives sold over online auction sites such as eBay are proving a valuable yet cheap source of confidential corporate data according to research carried out by Pointsec Mobile Technologies.

Pointsec discovered that 7 out of 10 hard drives bought over the Internet for around five British pounds each - less than the price of a fast food meal - still contained confidential information which could leave their former owners in breach of European data protection laws. The worst case involved a hard drive belonging to one of Europe's largest financial services organisations which contained pension plans, customer databases, financial data, payroll records and access codes for the company's Intranet.

Part of the problem is that confidential data on hard drives is not being adequately deleted before being sold on. But the Pointsec research also highlighted the fact that laptops mislaid at airports are often sold on to auction sites if they are not claimed by their owners. In many cases, simple password recovery software allows easy access to data stored on the hard drives.

Commenting on the research, Peter Larsson, CEO of Pointsec, said: "These findings show how important it is to never let laptops or mobile devices leave the office without being adequately protected with encryption and strong password protection."

To combat this problem, Pointsec recommends four key steps:

- Manage mobile IT security centrally rather than relying on employees to manage the problem.
- Ensure that access control and encryption is mandatory.
- Create a mobile usage policy with security guidelines and provide adequate training for staff.
- Deploy hard disk encryption that can provide protection beyond the life cycle of the laptop.

Canadian firms outstrip US on compliance

New research published by the Privacy Commissioner for Ontario has shown that Canadian companies tend to employ more robust privacy programmes that their US counterparts. The study, carried out by the US-based Ponemon Institute, looked at the practices of 19 Canadian and 19 US companies across areas such as policy, training, privacy and security management, and marketing choice.

Interestingly, while Canada has a stronger regulatory system in place, it was US companies that tended to view privacy from a risk management/ compliance perspective. Canadian companies, on the other hand, were more likely to recognise the commercial benefits of having robust privacy practices. 70 per cent of those surveyed drew a direct relationship between good privacy practices and customer trust and brand loyalty. Only 36 per cent of US companies, on the other hand, indicated a similar view.

The study also found that Canadian companies are more likely to employ privacy officers, who have greater sway with the CEOs or board of directors. Canadian companies are also more likely to offer greater privacy choices to their customers, provide awareness training for staff, and have systems in place to meet global privacy requirements.

For a copy of the study: www.ipc.on.ca/docs/cross.pdf

Financial firms improve on privacy compliance ...but there's still work to do

More financial service organisations are responding to growing privacy concerns by implementing stronger privacy practices, according to a survey published by Deloitte & Touche in May. The annual Global Security Survey 2004 questioned senior IT executives from top financial institutions on a range of issues including privacy and security, corporate governance, technology, budgets, and risk response.

The survey found that the number of organisations with a formal programme for managing privacy compliance has risen 20 per cent in the last year. However, this still only represented 67 per cent, a figure that seems relatively low for a sector that should really be in the vanguard of privacy protection.

Other areas of compliance did show improvements. 91 per cent of respondents had written privacy policies or data collection statements compared to 76 per cent the year before (see below).

Nearly half of organisations surveyed indicated that their approach to privacy was based on 'risk avoidance'. 29 per cent based their approach on compliance and legal responsibilities, while 25 per cent focused on brand and reputation.

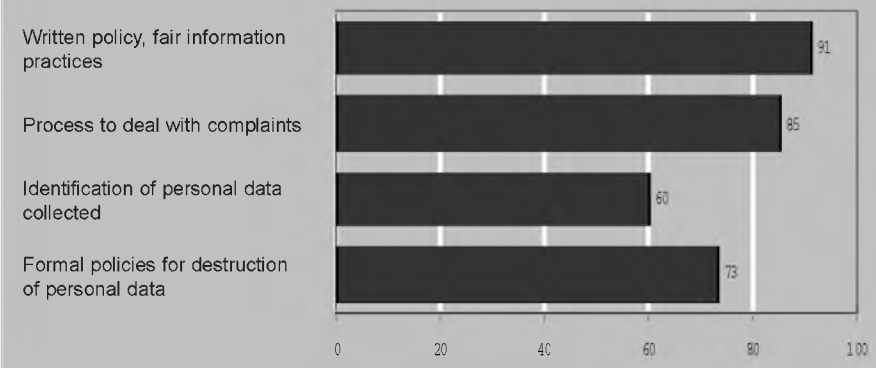
The survey did point out one possible area of concern, noting that a significant number of companies are incorporating privacy compliance into their information security functions. "Less than half the respondents," notes the survey, "has the protection of customer data under the control of the chief privacy officer."

Rather than creating a separate privacy programme, some financial institutions are handing responsibility for data protection to their chief security officers. Data privacy is also merged in with the companies' security policies, processes, and compliance programmes.

"The difficulty with this approach," the survey states, "is that security and privacy have their own objectives, their own goals and their own requirements - differences that dictate the need for the two areas to be examined separately."

A copy of the survey can be found in the Enterprise Risk section of Deloitte's website: www.deloitte.com.

Privacy Initiatives in Place



Source: Deloitte & Touche

eBay tops consumer privacy poll

Online auction giant, eBay, is the most trusted company for privacy protection according to a study carried out by the Ponemon Institute and online trust-mark provider TRUSTe.

The study, which polled over 6,300 US consumers, found that banks, healthcare and technology companies tend to outperform the retail and hospitality sectors when it comes to promoting good privacy values.

The study revealed that privacy-related issues form two of the top three components in establishing trust with consumers. Although a company's reputation for product and service quality ranked the most influential factor for consumers, the study found that ethical marketing and limiting the collection of personal data were also key factors.

Responding to the study, Scott Shipman, eBay's chief privacy officer, said: "Privacy is a key component of trust, which is crucial to the success of the eBay marketplace."

Larry Ponemon of the Ponemon Institute, said the study highlighted how privacy is increasingly being tied into the corporate brand. "Because consumers are becoming more concerned about identity theft and the safeguarding of their personal assets, a low privacy trust score could provide companies with an early warning signal that their reputation and brand loyalty might be in jeopardy."

Top ten privacy performers

1. ebay
2. American Express
3. Procter & Gamble
4. Amazon.com
5. Hewlett-Packard
6. US Postal Service
7. IBM
8. EarthLink
9. Citibank
10. Dell

Source: Ponemon Institute/TRUSTe

events diary

Privacy Laws & Business' 17th Annual International Conference
July 5-7, Cambridge, UK
The focus of this year's conference is how to integrate privacy into your business strategy. 50 speakers representing regulatory authorities, the European Commission, privacy managers and industry groups will address key issues such as outsourcing, compliant marketing, employee privacy and regulatory developments.

A full conference programme is available via our website. See: www.privacylaws.com/whats-newframe.htm

European Privacy Officers Network
July 8, Cambridge, UK
Includes a half-day session on Binding Corporate Rules, with a presentation on how the scheme is being adopted by companies in the Netherlands. The afternoon session will cover outsourcing, inspections/audits by DP authorities, and access rights.
Contact: Glenn Daif-Burns, Privacy Laws & Business
Tel: +44 (0) 208 423 1300
E-mail: glenn@privacylaws.com
Website: www.privacylaws.com/whats-newframe.htm

26th International Conference on Privacy and Personal Data Protection
September 14-16, Wroclaw, Poland
This year's annual conference for national privacy commissioners is being hosted by the Polish Data Protection Authority. Open sessions will cover a range of private sector concerns including RFIDs, biometrics and online privacy.
Contact: Polish Data Protection Authority
E-mail: privacy2004@giodo.gov.pl
Website: http://26konferencja.giodo.gov.pl/rejestracja/j/en/

Privacy Laws & Business Workshops

The Data Protection Act Explained - Basic Training for Beginners
September 21 - London; October 26 - Glasgow; December 7 - London
Privacy Laws & Business consultant, Valerie Taylor, presents a series of training workshops aimed at anyone who requires a basic course explaining the fundamentals of the Data Protection Act.

How to use the Information Commissioner's Data Protection Audit Manual
July 6-7, 2004 - Cambridge
PL&B is conducting a series of interactive audit workshops across the UK or available in-house. Visit our website to find out about future workshops.

Contact: Glenn Daif-Burns, Privacy Laws & Business
Tel: +44 (0) 208 423 1300
E-mail: glenn@privacylaws.com
Website: www.privacylaws.com/whats-newframe.htm

If you have an event or conference you would like listed, please contact Alan Pedersen at: e-mail alan@privacylaws.com.