Airline cleared over alleged privacy breach

The US Department of Transportation (DOT) has dismissed a complaint accusing Northwest Airlines of violating a privacy policy that promised not to sell customer data to third parties.

The Electronic Privacy Information Centre (EPIC) lodged the complaint in January this year after reports accessed under the Freedom of Information Act revealed that Northwest had passed customer data on to a NASA-backed anti-terrorism research project. EPIC argued that Northwest had engaged in unfair and deceptive trade practices because its privacy policy stated that customer details would only be shared in specific and limited circumstances. EPIC's complaint argued it was likely that "customers were misled by NWA's [Northwest Airlines] privacy commitment...to believe that their information would not be disclosed to third parties".

The DOT, which is tasked with regulating business practices in the transportation sector, has since cleared Northwest of any wrongdoing. In a report published September 10th, the DOT rejected EPIC's arguments, concluding that Northwest's privacy promises did not preclude it from sharing data with federal agencies, and that it was "required by law to make such records available…upon demand." The report added that there was no evidence of actual or likely harm to these passengers who provided Northwest with the data it shared."

The Northwest incident is one of a number of post-September 11th incidents involving the disclosure of customer details for national security-related projects. In June, a class action lawsuit launched against Northwest on similar grounds was thrown out. One of the reasons behind the decision was that customers had not actually read the airline's privacy policy.

EPIC is now calling for a review of the DOT's decision.

Lloyds TSB challenged over legality of data transfers

Trade union officials are questioning whether Lloyds TSB is breaching the UK Data Protection Act by outsourcing back office and call centre operations to India. Lloyds TSB Union (LTU), which is campaigning against the loss of UK jobs to foreign competition, confirmed in August that it had contacted the Information Commissioner "raising certain legal issues" over the transfer of customer data to a country which currently does not provide adequate legal protection for personal data.

A spokesperson for the union said that following advice from law firm Bindmans, the LTU is arguing that Lloyds customers "should be giving express consent if sensitive personal information is sent outside the EC [European Community]." Data protection experts, however, stress that consent is only one of a number of options that can be used to transfer data overseas.

Lloyds has expressed confidence that it is compliant with the UK Data Protection Act, arguing that "as long as we have measures in place to ensure an adequate level of protection for personal data, we are not required to obtain customers' explicit consent."

Penny Berryman, senior data protection manager for Lloyds, told *Privacy Laws & Business* that the bank has implemented a range of safeguards to ensure adequate protection, including contractual agreements that "closely follow" the standard processing contracts approved by the European Commission. She added that the bank has carefully assessed its outsourcing partners, ensures that customer data is stored on UK servers, and implemented detailed security provisions including clear desk policies, audit trails on data access, and onsite oversight from Lloyds TSB staff.

The Information Commissioner's office has so far declined to comment specifically on the case.

US drugstore chain accused of illegal data sharing

In September, civil liberties group, the Privacy Rights Clearinghouse, announced it had filed a lawsuit in California's Superior Court against Albertsons, a leading US supermarket and drugstore chain.

The Privacy Rights Clearinghouse is claiming that Albertsons violated customer privacy by selling prescription information to pharmaceutical companies without their consent. A number of top pharmaceutical companies have been named in the lawsuit, including Eli Lilly, Schering-Plough, AstraZeneca and Pfizer.

According to the lawsuit, Albertsons' customers received direct mail and telemarketing calls which were targeted according to confidential medical information that they disclosed to the drugstore chain.

Jeffrey Krinsk, a lawyer representing the Privacy Rights Clearinghouse, said that "the practices of Albertsons' drug marketing programme not only violate state safeguards of medical confidentiality, but intrude on consumer privacy while breaking the law…We will ask the Court to declare these practices illegal and enjoin Albertsons from using this marketing practice."

Albertsons has denied the accusations and said it will defend itself against the claims.

Further information: www.privacyrights.org/ar/PharmRelease.htm

IT security enjoys greater corporate recognition

IT security budgets have remained static over the last year, but companies are taking the issue more seriously, according to the results of a survey commissioned by *PricewaterhouseCoopers and CIO Magazine*. The State of Information Security Survey 2004, questioned 8,100 IT security professionals from 61 countries on developing trends in IT security. The survey found that security spending has plateaued, averaging out at around 11 per cent of the total IT budget. But, security is enjoying a higher profile within organisations with respondents citing the creation of more senior security roles with better reporting lines to senior management.

The key focus for security professionals in 2004 has been staff training, implementing disaster recovery programmes and establishing security policies. According to the survey, 92 per cent of organisations now have a formal IT security policy, but only 37 per cent have reviewed and measured the effectiveness of the policy.

Interestingly, Europe appears to lag behind other global regions when it comes to best practice security. Only 36 per cent of European respondents said that acceptable Internet usage policies had been incorporated into their overall security policies, compared to 58 per cent in North American organisations, and 41 per cent in the Asia-Pacific region. Only 40 per cent of European organisations' security policies addressed data protection issues such as disclosure and destruction of information, compared to 51 per cent in North America.

Further information: www2.cio.com /research/surveyreport.cfm?id=75

Insurance firm brings 'big brother' to the road

In August, UK insurance firm Norwich Union launched a new pilot scheme to track and record drivers' whereabouts. The "Pay As You Drive" project aims to provide customer-tailored motor insurance, calculating motorists' premiums based on where, when and how often they drive.

Norwich Union are currently fitting 5,000 telematic devices into volunteer customer cars as part of a two-year pilot scheme. The devices are similar to the 'black box' recorders used in aircraft, and will be able to monitor vehicle movement, locate stolen cars and, in the future, provide instant notification of accidents to insurers.

Concerns, however, have been raised over the privacy implications. A spokesman for human rights group Liberty told the *Sunday Herald*, "With any collection of data we must ask if there are legitimate reasons for collecting it, who gets access to the data and why?"

One major concern, if the project does get the commercial go ahead, would be the implications for staff driving company or hire cars and possible breaches of UK data protection law. Although most drivers may be required to consent to the use of this technology, there would be concerns over the rights of workers, and the extent to which employers would be able to access and use the data collected by these devices.

News in brief

SECURITY BREACH - In September it was revealed that the University of California had discarded a laptop hard drive containing personal data on around 23,000 people. The data, belonging to staff and students, included names, addresses and social security numbers.

According to *Computerworld*, Californian security laws enacted last year have required the university to inform all affected people that their details have been compromised.

MOBILE SECURITY - According to the Mobile Vulnerability Survey 2004, two thirds of corporate PDAs used for storing confidential data are not being adequately protected with encryption. The survey, conducted by Pointsec and Infosecurity Europe found that while PDAs are increasingly being used to access e-mail or store client data, businesses are not taking sufficient steps to protect the information from unauthorised access.

While the percentage of companies which have established mobile security policies has increased to over 50 per cent (from 27 per cent in 2003), those enforcing the policy through proper security controls has remained static.

ID THEFT - In September, a former employee of US firm, Teledata Communications (which provides financial services firms with access to consumer credit data) pleaded guilty to fraud charges in what has been described as the largest case of identity theft in the US.

According to *Computerworld*, Philip Cummings, a help desk worker at Teledata, helped to steal the information on up to 30,000 consumers, which was then used to set up bogus credit card accounts. Cummings is due to go on trial in November this year.

Data security a priority for global outsourcing

Analysts speaking at Gartner's IT Security Summit in London this September have warned that data security is set to take centre stage as a key outsourcing issue.

As offshore outsourcing models become increasingly complex, the cost and exposure through security breaches is expected to rise. "The security exposure that both clients and service providers have to deal with, as global sourcing becomes more strategic and complex, increases by orders of magnitude," said Partha Iyengar, Research Vice President for Gartner India.

To minimise the risks, Iyengar stressed that there must be greater cooperation between enterprises and service providers in order to effectively manage the risks. "Service providers and users need to look jointly at risk and work together to create an information protection framework to identify and spell out each of the concerns, determine their validity and make educated decisions about the risk they may or may not pose," said Iyengar.

He added that to minimise the increasing costs of security compliance, businesses will need to carry out thorough risk assessments on the types of information being outsourced overseas. "Diligence in understanding the actual risks involved will ensure that educated decisions can be made on the ROI around security expenses and investments," he said. "Certain companies and vertical industries will have to classify data or determine the requirements for sharing data on a project by project basis."

FTC tackles online privacy violation

In July, Gateway Learning, a US-based provider of children's educational tools, was brought to task by the Federal Trade Commission (FTC) for violating its online privacy policy. Gateway, which operates under the 'Hooked on Phonics' brand, rented out customer details to third party marketers despite pledging that it would not share information without their consent.

Although Gateway altered its privacy policy in 2003 to reflect its data sharing practices, the FTC claims that data collected under the previous policy was still rented out - despite promises that customers would be informed of any material changes to the policy and be offered the chance to "opt-out" from having their details shared with third parties.

In settling the FTC charges, Gateway agreed to pay out the roughly $4,500 it earned from renting out the customer data. The settlement also requires the company to get consent from customers whose details were collected under the original policy before it shares their data with other companies.

Commenting on the case, Howard Beales, director of the FTC's Bureau of Consumer Protection said: "It's simple - if you collect information and promise not to share, you can't share unless the consumer agrees. You can change the rules, but not after the game has been played."