Amazon accused of child privacy violations

Towards the end of April, US consumer groups petitioned the Federal Trade Commission (FTC) to investigate alleged breaches of the Children's Online Privacy Protection Act (COPPA) by online retailer Amazon. The COPPA law applies to any online businesses targeted at children, or knowingly collecting information from them. Businesses are required to post privacy policies, get verifiable parental consent when collecting data from under-13s, allow parents to access their children's details and block any further processing.

Already this year, there has been significant enforcement action taken against child-orientated sites. In February, the FTC imposed record penalties on Mrs Fields Cookies and Hershey Foods ($100,000 and $80,000 respectively) for COPPA violations (*PL&B International*, March/April 2003, p.16).

Although Amazon sells children's toys through its website, it claims that it is not required to comply with COPPA as it does not market products at children. The company's privacy policy states: "Amazon.com does not sell products for purchase by children. We sell children's products for purchase by adults. If you are under 18, you may use Amazon.com only with the involvement of a parent or guardian."

However, consumer groups (including the Electronic Privacy Information Centre, the Centre for Media Education, and Junkbusters) argue that Amazon falls under the scope of COPPA on two counts. Firstly, they state that the "Toy Store" section of Amazon's website is clearly targeting children. Secondly, they allege that Amazon is knowingly collecting children's details through its product review section. Children and adults are able to post reviews of games, books, music etc. on Amazon's website after registering their details. Although Amazon's site does have a separate "Kid's Review Form", allowing children to post anonymous reviews, consumer groups claim that the hyperlink to the form was often not working, forcing children to posted reviews via the adult section [Amazon has since announced that it has fixed the link].

Consumer groups claim a statement by Amazon that it screens product reviews is proof that the company is knowingly collecting information from under-13s. It cites cases in which childrens' names, ages, gender, e-mail and postal addresses have been posted online.

In response to the accusations over Amazon's privacy practices, the FTC stated that it will look into the consumer groups' claims, but has not confirmed whether it intends to launch a formal investigation. Amazon has continued to deny that it needs to comply with the COPPA regulations. A spokesperson for the company told the *Washington Post*: "We are not a site that's directed at children. We're a store. We sell things, and you need a credit card to buy them. When it comes to reviews, we created special software for anonymous reviews by children under 13."

New York hotel feels wrath of privacy activist

The management of one New York City hotel is tending its wounds after butting heads with a determined American privacy activist. To make matters worse for the management, a recounting of their security imbroglio, complete with an embarrassing audio file, is now posted on the Internet, along with a call by the activist for a worldwide boycott of the Ramada hotel chain.

Mike Stollenwerk of the Fairfax County Privacy Council had travelled to New York to attend the April 2003 Computers, Freedom and Privacy conference. He had made a credit card reservation for his hotel room. On his arrival late in the evening, he presented his credit card but was told he must present photo ID. Stollenwerk refused. After an hour of heated discussions with hotel staff, Stollenwerk presented his voter registration card (which had no photo). The receptionist photocopied these documents, and he was then allowed to go to his room (He was later told that the hotel would keep these photocopies for about 30 days).

The next day, Stollenwerk received a message asking him to meet with the hotel security director. At that meeting, citing legal precedents, Stollenwerk explained his objections to presenting photo ID and having it photocopied.

The tale did not end there. Returning to his room after the day's conference, Stollenwerk found the following message on his voicemail: "This is Barry Mann, General Manager of the hotel, Mr Stollenwerk. Ahhh, it's a little after nine in the morning. I'd like you to come down and present some picture ID. Otherwise, the next knock on the door will be the police terrorism squad. Thank you."

The police terrorism squad never did appear. And Stollenwerk had the presence of mind to consult with his conference colleagues and record the manager's message on a digital recording device. The audio file of the manager's message is now posted on the Internet.

Says Stollenwerk: "[N]ow I know why New York City is the 'city that never sleeps' - because you can't sleep in New York City hotels unless you have Photo-ID and let the hotel copy and retain it."

Report by Eugene Oscapella

The audio file containing the manager's "terrorism squad" warning, and Stollenwerk's diary of the encounter, can be found at: http://www.privacyrights.org/ar/NYRamada.htm

European e-tailers weak on privacy

A survey published in April by IT World Lawyers has revealed that online businesses in Europe are failing to comply with data protection legislation. The survey, carried out by IWD Market Research, looked at a total of 420 websites across seven countries which sell a range of products such as electronics, books, and holidays. It found that only around half of the websites studied contained some form of privacy policy or data protection statement.

Results showed that while the UK leads Europe in terms of transparency (71.7 per cent of UK sites posted a privacy policy), France lagged well behind with only 31.7 per cent bothering to communicate their privacy practices.

More worryingly, only a quarter of the 420 websites gave consumers the option to opt-out from direct marketing. Portugal topped the table in this category with 35.3 per cent providing an opt-out, while Germany and Spain bottomed-out at 18.3 per cent.

The survey also revealed non-compliance with other e-business legislation. Only 29.7 per cent, for example, complied with the EU Distance Selling Directive by informing consumers of their right to withdraw from a contract within seven days. Additionally, around 40 per cent failed to provide an electronically available version of their standard business terms.

The countries included in the survey were: France, Germany, the Netherlands, Portugal, Spain, Switzerland, and the UK.

Global businesses face tighter controls over data transfers

A new data protection survey has shown that global businesses face an increasingly complex set of obstacles when transferring data between countries. The 2003 Data Protection Survey, published by White & Case in conjunction with the law firm's Global Privacy Symposium last month, specifically looked at how divergences in privacy laws are preventing the free flow of information across borders.

The survey examined 22 key jurisdictions from Europe, the Asia-Pacific region, and North America (including four non-sovereign states - California and New York in the US, and Ontario and Quebec in Canada).

Key findings revealed that most of the jurisdictions surveyed place some degree of restriction on cross-border transfers and that the EU Data Protection Directive is emerging as a benchmark by which jurisdictions measure their data transfer procedures.

12 of the 22 jurisdictions surveyed place restrictions on data transfers with another five (Hong Kong, Malaysia, Mexico, Thailand, and Ontario) considering proposals to do so. But, the survey found discrepancies in the way these 12 jurisdictions handle cross-border data flows.

All 12, for example, allow the use of customer or employee consent to legitimise data transfers. However, nine operate an opt-in approach to consent, while Australia, the UK and Quebec allow consent to be gathered on an opt-out basis.

9 of the 12 jurisdictions surveyed allow data transfers in cases where it is necessary to protect the vital interests of the individuals concerned, but only four jurisdictions have approved a standard contract for cross-border transfers.

Robert L Raskopf, head of the IP and E-commerce, Media and Technology practice groups at White & Case, summed up the complexities facing businesses by using the example of data flows between Australia and Spain. An Australian-based business, he said, would be permitted to export personal data to Spain if it were necessary to protect individuals' vital interests, but transferring information from Spain to Australia under the same circumstances would not be allowed.

Similarly, while Spain would allow information to be transferred to Australia in the context of defending a legal claim, the reverse process would again be prohibited.

For a copy of the White & Case 2003 Data Protection Survey, see: www.whitecase.com

Jurisdictions surveyed were:

EUROPE	ASIA-PACIFIC	NORTH AMERICA
France*	Australia*	Mexico
Germany*	China	Canada*
Hungary*	Hong Kong	United States
Italy*	Japan	Ontario
Poland*	Malaysia	Quebec *
Russia*	South Korea*	California
Spain*	Thailand	New York
United Kingdom*		

(Jurisdictions which restrict cross-border data transfers)*

News in brief

CORPORATE PRIVACY

US Internet service provider, Verizon, is to hand over the names of four anonymous customers who have been accused by the Recording Industry Association of America (RIAA) of illegally swapping music files. On June 4th, the US Court of Appeals for the District of Columbia backed earlier judgments forcing Verizon to comply with disclosure subpoenas issued last year by the RIAA under the Digital Millenium Copyright Act.

Earthlink has been awarded $16.4 million (€14 million) in damages after a New York-based spammer sent 825 million spam e-mails through the US-based Internet service provider's servers. According to *NewsFactor.com*, Earthlink also won $25 million (€21 million) from a Tennessee-based spammer in 2001 - although it has yet to receive any payment.

According to the 2003 Global Security Survey published by Deloitte Touche Tohmatsu, consumer expectations play little part in organisations' decision to implement good privacy practice. While 90 per cent of respondents cited legal and industry regulations as a key driver for getting privacy compliant, only 47 per cent considered the privacy expectations from their customers to be an influencing factor.

IT analyst firm, Gartner, says US companies that fail to implement robust privacy practices risk customer backlash and could force the government into creating further privacy legislation. Walter Janowski, research director at Gartner, said: "In a climate in which the general public is greatly concerned with corporate ethics and accountability, a business that makes a significant misstep in managing its customers' private information could have a highly visible and damaging public scandal...If US businesses don't prioritise privacy management, public outcry will motivate the US Congress to mandate restrictive privacy legislation."

EU 'corporate rules' report published

On June 4th, the EU Article 29 Data Protection Working Party published a report on proposals to allow the use of 'binding corporate rules' for international data transfers. Multinational companies such as BP, Shell and Accenture are already trialing the scheme which aims to ease restrictions on data exports outside the EU (see *PL&B International*, March/April, p.1).

The Working Party proposals envisage organisations creating a single legally binding privacy policy that would then be approved by EU data protection authorities.

Conditions for authorising the use of the 'corporate rules' scheme would require companies to not only train their staff in data protection, but also demonstrate good levels of awareness within the company. The scheme would also require regular privacy audits supervised by external auditors. Companies would be required to submit the results to data protection authorities and act on any advice or recommendations given.

Companies would also have to set up proper complaints handling procedures, inform employees and customers of their privacy practices and details of international data transfers. Individuals would be able to take legal action, not only in their home country, but also in the country in which the company has located its headquarters (provided it is in the EU). Companies would be required to demonstrate that they have sufficient assets to cover any compensation that might arise as a result of a privacy breach.

The Working Party has stressed, however, that the corporate rules scheme will not necessarily be the correct approach for all organisations. "For loose conglomerates," says the report, "binding corporate rules are very unlikely to be a suitable tool." The Working Party also states the scheme "should not be considered as the only or the best tool for carrying out international transfers," but rather as an additional option in situations where other methods (such as the European Commission's standard contractual clauses) "seem to be particularly problematic."

For a copy of the Working Party's report, see: http://europa.eu.int/comm/internal_market/privacy/workingroup/wp2003/wpdocs03_en.htm

Ireland amends DP law

On April 10th, Ireland passed the Data Protection (Amendment) Act 2003. The changes have been incorporated into the existing 1988 Act. The amendments bring Ireland into line with the EU Data Protection Directive and come nearly five years after the deadline for transposing the directive - Ireland was in fact prosecuted in the European Court last year for the delay (*PL&B International*, June 2002, p.9).

The new amendments come into force on July 1st and include provisions on manual data, sensitive personal data, the use of public registers for marketing, and strengthened rights over access to data. A guidance document to help organisations comply with the new law has been published on the Data Protection Commissioner's website.

Meanwhile the Commissioner, Joe Meade, has published his annual report for 2002. Figures show that complaints are down nearly 20 per cent from 233 in 2001 to 189 last year. However, complaints are still significantly higher than the 131 received in 2000, and could rise again because of the Commissioner's plans to launch a public awareness campaign over the coming year.

The majority of complaints were against the financial services industry (24 per cent) and the telecoms sector (16 per cent). Most of the complaints that were lodged concerned access to personal data (30 per cent) and direct marketing (29 per cent).

See p.18 for more details on the Data Protection (Amendment) Act 2003.

Dutch DPA pledges support for industry codes of practice

According to its annual report for 2002, the Dutch Data Protection Authority (CBP) has made significant progress in promoting self-regulation among private sector organisations. During 2002 it formally approved the first industry code of practice for companies involved in pharmaceutical research. And, in January this year, a second code governing the financial sector was approved.

Three more codes - covering private investigators, court bailiffs and employment agencies - are expected to be approved this year. However, talks between the CBP and representatives from 'trade information agencies' (which process credit/debt information) for a code of practice have reportedly stalled. The CBP has labelled compliance within the sector as "thoroughly unsatisfactory" and has pledged to take a firmer line in the future. "The best solution," it says, "is likely to lie in further regulations on the way personal data is obtained for credit rating and debt collection purposes."

The CBP's report also details other efforts to promote self-regulation. Progress has been made in efforts to develop a data protection auditing scheme for organisations. In response to consultation with accreditation firms, the CBP has agreed upon a scheme for accrediting privacy auditors. Already, a number of organisations have agreed to act as accreditation bodies which will be responsible for approving privacy auditors. These auditors will then be empowered to issue organisations with certificates for good privacy compliance.

Along with efforts to promote good compliance, the CBP has also been stepping up its enforcement activities. During 2002 it set up a new department dealing specifically with complaints appeals, and created a new enforcement strategy. One of the initial target areas for enforcement is organisations which have not notified their processing operations with the CBP.

For a copy of the CBP's annual report see: www.cbpweb.nl

Italian privacy complaints are on the rise

Official complaints from individuals over violations of their privacy have risen nearly 60 per cent over the last year, according to the Italian Data Protection Authority. Figures published in its annual report show that there were 3,689 complaints in 2002 compared to 2,327 the year before. Additionally, the authority dealt with 12,800 requests for information on data protection issues.

Many of the complaints were focussed on unsolicited e-mail marketing. An investigation launched by the authority earlier this year revealed that many organisations were illegally collecting e-mail addresses by harvesting them from public areas of the Internet. The authority has stressed the need for a clearer legal framework on the use of personal data over the Internet.

The report revealed that the number of settled legal actions has more than doubled, from 211 in 2001 to 500 in 2002. Most cases, according to the authority, involved data protection breaches in the telecoms sector.

The authority has also stepped up its enforcement activities, doubling the number of official investigations to 40 in 2002.

A copy of the annual report for 2002 can be found at: www.garanteprivacy.it/garante/navig/jsp/index.jsp

Swedish e-tailers unaware of privacy rules

Swedish e-businesses have poor data protection knowledge, according to a report from the Swedish Data Protection Authority (DPA). The report, published in May, found that many companies are not familiar with even the most basic privacy principles.

The DPA investigated the privacy practices of 46 randomly chosen e-commerce companies after having received a number of complaints. The companies represented the travel, health and leisure sectors, and included well-known brand names such as IKEA and SAS.

Of those interviewed, only 12 identified themselves as data controllers. Information given to individuals about access and the purposes for which their data will be used was insufficient. Half of the respondents did not provide any information, and only two complied fully with the law's requirements in this respect.

All of the respondents used customer data for marketing purposes, and one third also forwarded address details on to business partners and other third parties. Rules on data security were generally not well known. Many of the respondents had not carried out any kind of risk assessment. Companies also lacked processes to destroy unnecessary personal data. Half of the respondents never destroyed any personal data. Some of those which destroyed unnecessary data only did so every six years.

The Swedish Data Protection Act requires data subjects' consent for the processing of sensitive data as well as, in most cases, for the processing of ID-numbers. One third of the respondents stored individuals' ID-numbers on their systems.

The DPA has published the findings (in Swedish) on its website www.datainspektionen.se, along with tips for e-commerce companies on how to comply with the Data Protection Act. The authority plans to carry out further compliance checks in the future.

Report by Laura Linkomies.

UK publishes workplace privacy code

On 11th June, the UK Information Commissioner published its long-awaited code of practice on employee monitoring. The code is the third in a four-part series dealing with a variety of data protection issues in the workplace.

While it is not legally binding, there are fears that employment tribunals could refer to the code when making their judgments.

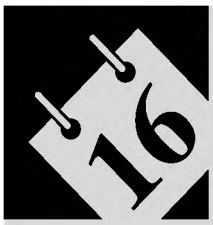
The code applies to a number of potentially invasive practices including monitoring e-mail and Internet use, CCTV/video surveillance, vehicle tracking technologies, and using third parties such as private detectives to monitor employees.

Key guidance in the code includes creating 'impact assessments' to judge whether monitoring is necessary, delegating monitoring responsibility to trained staff, promoting staff awareness of monitoring practices, and avoiding snooping into workers' personal correspondence.

Information Commissioner, Richard Thomas, commented: "If any monitoring is to take place, it must be open and transparent and with the knowledge of the employee. In reality there are few circumstances in which covert monitoring is justified."

A copy of the "Monitoring at Work" code is available from the Information Commissioner's website: www.dataprotection.gov.uk/dpr/dpdoc.nsf.

The final section of the workplace privacy code, covering medical testing and health data is expected to be published at the end of this year.



events diary

Privacy Laws & Business 16th Annual International Conference - Transforming Risk Assessment Into Everyday Compliance with Data Protection Law
July 7-9, Cambridge
This year's event features 46 speakers from 7 countries, including the regulatory authorities from the United Kingdom, the Netherlands and Hong Kong, in addition to a host of sessions on a wide range of both data protection and freedom of information issues.
Contact: Shelley Roche, Privacy Laws & Business
Tel: +44 (0) 208 423 1300
Fax: +44 (0) 208 423 4536
E-mail: shelley.roche@privacylaws.com
Website: www.privacylaws.com

The Body As Data
September 8, Melbourne, Australia
A one-day conference featuring a keynote address from Stefano Rodota, head of the Italian Data Protection Authority and chairman of the EU Data Protection Working Party. Presentations cover privacy implications on issues such as genetics and biometrics.
Contact: Office of the Victorian Privacy Commissioner
Tel: +61 3 8619 8719
Fax: +61 3 8619 8700
E-mail: conference@privacy.vic.gov.au
Website: www.privacy.vic.gov.au

Global Privacy Management
September 9, Sydney, Australia
A one-day conference intended to provide an opportunity to learn and share in the latest developments in privacy implementation across the world.
Contact: Tim Dixon, Australian Corporate Privacy Officers' Network
Tel: +61 2 9225 1564
E-mail: mail@cpo.net.au
Website: www.cpo2003.com

25th International Conference of Privacy and Data Protection Commissioners
September 10-12, Sydney, Australia
The theme for this year's annual conference is 'Practical privacy for people, government and business' and features presentations from privacy commissioners and representatives from the public and private sectors and other interested groups.
Contact: Tour Hosts Conference & Exhibition Organisers
Tel: +61 2 9248 0800
Fax: +61 2 9248 0894
E-mail: privacy2003@tourhosts.com.au
Website: www.privacyconference2003.org

The Data Protection Act Explained - Basic Training for Beginners
September 24 - London; October 29 - Bristol; November 26 - Edinburgh; December 17 - London
Privacy Laws & Business consultant, Sandra Kelman, presents a series of training workshops aimed at anyone who requires a basic course explaining the fundamentals of the Data Protection Act.
Contact: Sandra Kelman, Privacy Laws & Business
Tel: +44 (0) 208 423 1300
Fax: +44 (0) 208 423 4536
E-mail: sandra@privacylaws.com
www.privacylaws.com/whats-newframe.htm

How to use the Information Commissioner's Data Protection Audit Manual
July 8-9 - Cambridge; September 15-16 - London
Privacy Laws & Business is conducting a series of two day interactive audit workshops across the UK or in-house.
Contact: Shelley Malhotra, Privacy Laws & Business
Tel: +44 (0) 208 423 1300
Fax: +44 (0) 208 423 4536
E-mail: shelley@privacylaws.com
Website: www.privacylaws.com/whats-newframe.htm