Yahoo! settles marketing investigation

Internet portal, Yahoo!, has agreed to pay $75,000 (€64,000) in costs and make substantial changes to its marketing practices following a settlement with the New York State Attorney General's office.

The Attorney General, Eliot Spitzer, initiated the investigation after Yahoo! revised its privacy policy in March last year, effectively resetting customers' privacy preferences and allowing it to start marketing to them across a range of channels such as fax, e-mail, phone and post. Although customers were sent an explanatory e-mail giving them 60-days to opt-out from the new marketing policy, Yahoo! failed to obtain positive consent, despite the fact that some customers had previously chosen not to receive marketing communications.

As part of the settlement, Yahoo! agreed to stop making telemarketing calls to customers who had previously opted-out from marketing contact. It will also provide consumers with clear notice of Yahoo!'s privacy practices in addition to a "clear and conspicuous" hyperlink to an online unsubscribe page, allowing customers to set their marketing preferences.

Commenting on the settlement, Spitzer said: "It is neither appropriate nor legally permissible for a company to compile a database of personal information through an online registration process and then attempt to use the information for telemarketing purposes to target consumers who have stated that they do not want to receive solicitations."

Privacy activists take protest to the sky

In late October, a California-based consumer group used a professional skywriter to disclose personal information about Citigroup CEO Charles Prince. The Foundation for Taxpayer & Consumer Rights (FTCR) revealed the first five digits of Prince's social security number above Citigroup's New York headquarters as a protest against a federal financial bill (S.1753 Shelby/Sarbanes) aimed at restricting consumer privacy rights. Citigroup was targeted by the group because of its strong lobbying influence behind the bill. Jerry Flanagan of the FTCR criticised Citigroup's support for the bill, saying "Banks should oppose, not support, the pending federal legislation."

Victoria's Secret pays out $50,000 for security breach

Secret by name, but not it seems by nature. Between August and November last year, over 500 customers of lingerie retailer, Victoria's Secret, literally had their underware aired in public after a security glitch on the company's website left their accounts exposed. Although no financial details were revealed, outsiders could gain access to customer names, addresses and purchase information.

Following an investigation by the New York State Attorney General's office, Victoria's Secret will pay a $50,000 (€43,000) penalty and tighten up its online security procedures.

The security flaw was discovered last year by Jason Sudowski, who inadvertently stumbled across customer records by simply by changing the online customer identification numbers.

According to the *New York Times*, Sudowski alerted Victoria's Secret to the problem but was told that nothing could be done. It was only after *MSNBC.com* reported the incident that the security glitch was finally fixed.

The security flaw appears to have violated the company's privacy and security policy, leaving it susceptible to claims that it broke state laws on deceptive practices. At the time of the incident, the privacy policy stated: "Any information you provide to us at this site when you establish or update an account, enter a contest, shop online or request information...is maintained in private files on our secure web server and internal systems..."

As part of the settlement with the Attorney General, Victoria's Secret will implement the following safeguards:

- establish and maintain an information security programme to protect personal information
- establish management oversight and employee training programmes
- hire an external auditor to annually monitor compliance with the security programme; and
- provide refunds or credits to all affected New York consumers.

Commenting on the settlement, Attorney General, Eliot Spitzer, said: "A business that obtains consumers' personal information has a legal duty to ensure that the use and handling of that data complies in all respects with representations made about the company's information security and privacy practices."

AT&T accused of breaching telemarketing rules

US telecoms giant, AT&T could be hit with a fine of up to $780,000 (€680,000) for breaching US telemarketing rules. The Federal Communications Commission (FCC), one of the government agencies tasked with regulating the recently introduced Do-Not-Call rules, has announced its intention to fine AT&T in what will be the first major case of its kind.

The US Do-Not-Call rules allow consumers and individuals to opt-out from unsolicited telemarketing by registering onto a federal list. Marketers that break the rules by calling people on the list can be fined $10,000 (€9,000) per violation.

The action was initiated after more than 300 complaints were made about AT&T's marketing practices. Following an investigation, the FCC now alleges that AT&T breached the rules by making unsolicited calls to 29 consumers on 78 separate occasions.

According to recent figures from the Federal Trade Commission, the number of phone numbers registered on the Do-Not-Call list have now topped 54 million. Already, 51,000 complaints have been made by individuals.

Study reveals privacy flaws in online financial services

A recent report carried out by IBM and Watchfire has revealed that over half of global financial organisations have privacy compliance gaps in their corporate websites. While financial organisations often lead global industry in terms of privacy protection and security, the rapid expansion of corporate websites, which can stretch across thousands of web pages, has increased the ease with which unforeseen compliance gaps can occur.

The study, carried out in September this year, looked at 242 financial services organisations listed in *Business Week's* Global 1,000 companies index. By scanning the companies' websites, IBM and Watchfire found that 53 per cent of the sites examined contained web pages that collected sensitive information, but failed to provide a link to the company's privacy policy. The study recommends that, at a minimum, hyperlinks to privacy policies should be "accessible at all data collection points."

Comprehensive security across the whole of the corporate website is another issue that appears to have been overlooked by some financial organisations. The study found that 18 per cent of sites used data submission forms that could expose sensitive personal data (such as passwords, credit card details and postal addresses) to hackers and identity thieves.

66 per cent of sites had at least one submission form collecting sensitive data that failed to provide SSL (secure socket layer) encryption security. Two of the sites studied did not mask online passwords (eg. replacing keystrokes with asterisks) which could leave customers' susceptible to so-called 'shoulder surfing'.

The study also noted that very few companies had adjusted their websites to take account of the Platform for Privacy Preferences (P3P) standard, a technology that allows consumer web browsers to automatically identify and verify online privacy practices. Only four per cent of sites had implemented a full P3P compliance policy, while two per cent had implemented a compact P3P policy (which sets out the website's policy on the use of cookies). This is despite the fact that 93 per cent of sites were using 'persistent' cookies which could be blocked by consumers using the P3P tools available in web browsers such as Internet Explorer 6.0.

A copy of the IBM/Watchfire report, can be found at:
www.watchfire.com/resources/state-online-finance.pdf

Radio frequency identification project under fire

A November 10th article in the *Chicago Sun Times* reported that shoppers in an Oklahoma store of American retail giant Wal-Mart were unwitting guinea pigs earlier this year in a secret study that employed Radio Frequency Identification (RFID) technology and surreptitious camera surveillance.

The newspaper reported that shelves in the store were equipped with hidden electronics to track the lipstick containers on them and that the shelves and webcam images were viewed by Procter & Gamble researchers hundreds of miles away in Cincinnati. Researchers could tell when lipsticks were removed from the shelves and could watch consumers in action.

Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN), a grass-roots US consumer group fighting retail surveillance schemes, claims that customers who purchased the lipstick unknowingly left the store with live RFID tracking devices embedded in the packaging.

"This trial is a perfect illustration of how easy it is to set up a secret RFID infrastructure and use it to spy on people," says CASPIAN's founder, Katherine Albrecht.

Further information:
www.spychips.com/#scandal

India to water down privacy plans

The Indian government appears to be backing away from implementing a comprehensive data protection law, according to a report by the *Times of India*. In June this year, the Department of Information Technology announced that it had prepared a draft Data Protection Act based around the EU Data Protection Directive. The government has been under pressure from industry to implement privacy legislation that will make it easier for European companies to outsource their data processing operations to India.

However, the *Times of India* now says that a separate data protection law is unlikely and that any additional privacy regulation could be implemented through amendments to the existing Information Technology Act 2000. Instead of a comprehensive privacy law that meets European standards, the government is now expected to initiate dialogue with the European Commission with a view to establishing a Safe Harbor-style agreement that will lift the restrictions placed on the exchange of data between Europe and India.

European trade unions call for ban on genetics testing

The European Trade Union Confederation (ETUC) has called for an EU-wide ban on genetics testing in the workplace. Although there are relatively few examples of genetics testing in Europe, ETUC is concerned that the increasing use of genetics tests in the US could seep though into European workplace culture.

In a statement published in October, ETUC warned that genetics testing could "introduce discriminations amongst workers according to certain genetic characteristics" leading to "indirect forms of racial discrimination."

ETUC's position is supported by findings in a report published in July by the European Group on Ethics in Science and New Technologies (EGE), an independent advisory group to the European Commission.

The EGE concedes that genetics testing could benefit workers in areas such as health and safety. Tests could potentially be used to identify employees who are susceptible to certain workplace hazards. However, its report concludes that currently, it is "difficult to make a case for any genetic tests to be carried out as indicators of future health in terms of their relevance to employment."

The EGE warns that that there are presently few tests available that provide employers with enough information to be able to make valid employment decisions. It also states that links between workers' genetic status and their susceptiblity to workplace hazards has only a theoretical basis at present.

The fact that employers could be collecting data that presents a false or misleading picture on employees, suggests that genetics testing could conflict with key privacy principles such as proportionality and accuracy of information.

ETUC has pointed out that member states such as Austria, Belgium and Finland have already prohibited genetics testing in the workplace. But it now wants to see a harmonised approach, and has called for a ban to be incorporated into a new directive on workplace privacy being drafted by the European Commission.

A spokesperson for the Commission has said that while there is no firm timetable for introducing the directive, it could be presented to the European Parliament and Council towards the end of November this year.

For a copy of the EGE report: http://europa.eu.int/comm/european_group_ethics/docs/avis18EN.pdf

EU member states urged to improve data transfer authorisations

The European Commission has sent a "note" to EU member states and data protection authorities regarding improvements to the system of authorising data transfers to countries that do not provide adequate levels of protection. The Commission's action marks a step forward in its efforts to promote more effective and harmonised data protection regulation across the EU.

A review of the EU Data Protection Directive carried out in 2002 highlighted a number of shortcomings in data protection law, with data transfers proving to be a key area in need of reform. The Commission's report, published in May this year, stated that "many unauthorised and possibly illegal transfers are being made to destinations or recipients not guaranteeing adequate protection. Yet there is little or no sign of enforcement actions by the supervisory authorities."

The note to member states provides details on handling authorisations relating to contractual clauses and "binding corporate rules".

A copy of the European Commission's note can be found at: http://europa.eu.int/comm/internal_market/privacy/lawreport_en.htm

For a copy of the European Commission's review of the EU Data Protection Directive, see: http://europa.eu.int/eur-lex/en/com/rpt/2003/com2003_0265en01.pdf

British Columbia enacts private sector data law

British Columbia's Personal Information Protection Act is to come into force on January 1st 2004. It will apply to all private sector companies and contains rules to protect personal data collected, used and disclosed by organisations. The province's Information and Privacy Commissioner will oversee and enforce the new law.

British Columbia has become only the second Canadian province (Quebec was the first) to enact data protection legislation for the private sector. Alberta introduced similar legislation in May 2003, but it has not yet been enacted.

Canada's federal private sector data protection legislation, the Personal Information Protection and Electronic Documents Act, currently covers only the activities of federally-regulated commercial organisations. However, as of January 1st 2004, it will be extended to all companies, including provincially-regulated organisations, unless a province enacts legislation that is substantially similar to the federal act. The British Columbia and Alberta laws are intended to fufil the role of "substantially similar" legislation. This will leave commercial organisations in most provinces and territories, including Ontario, to be regulated under the federal act as of January 1st, 2004.

Successful E-marketing within the new E-Privacy Regulations
December 11th, London, UK
A one-day event examining the new E-Privacy Regulations which come into force on December 11th.
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

Subject Access in an Ongoing or Potential Dispute/Monitoring at Work
February 24, 2004, London, UK
PL&B presents a one-day conference covering subject access rights and workplace monitoring.
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

The Data Protection Act Explained - Basic Training for Beginners
December 17 - London
Privacy Laws & Business consultant, Sandra Kelman, presents a series of training workshops aimed at anyone requiring a basic course explaining the fundamentals of the Data Protection Act.
Contact: Sandra Kelman, Privacy Laws & Business
Tel: +44 (0) 208 423 1300
E-mail: sandra@privacylaws.com
Website: www.privacylaws.com/whats-newframe.htm

How to use the Information Commissioner's Data Protection Audit Manual
December 8-9 – London; February 9-10, 2004 – Leeds; May 10-11, 2004 – London; July 6-7, 2004 - Cambridge
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
E-mail: shelley@privacylaws.com
Website: www.privacylaws.com/whats-newframe.htm

WorldLII launches privacy research database

The World Legal Information Institute (WorldLII), which promotes free, independent and non-profit access to worldwide law, has recently announced the creation of a searchable privacy and freedom of information law database. The Privacy & FOI Law Project aims to make searchable from one location - at no cost - all of the databases specialising in Privacy and/or FOI law available on any of the Legal Information Institutes (LIIs) that are part of WorldLII. The current databases include the case reports/summaries available from eight FOI and/or Privacy Commissioners from Australia, Canada, Ireland and New Zealand, plus EPIC Alert and the Privacy Law & Policy Reporter archive. Individual databases may be searched on their respective host LIIs. More information will be added once permission is received to add them.

Privacy expert Graham Greenleaf, Professor of Law at the University of New South Wales, and Co-Director, Australasian Legal Information Institute (AustLII), is one of the driving forces behind the database. He has invited those using the web resource to provide feedback. He also states that proposals for inclusion of new resources are particularly welcome.

For details of the Privacy & FOI Law Project see: www.worldlii.org/int/special/privacy. Readers should also visit the main WorldLII website (www.worldlii.org) which lists other legal and privacy resources.

Canada's annual privacy report published

Canada's Interim Privacy Commissioner, Robert Marleau, released the Office of the Privacy Commissioner of Canada's 2002-2003 Annual Report on September 17th. The Annual Report discusses the Office's activities under two federal privacy laws. The Privacy Act covers the personal information-handling practices of federal government departments and agencies, while the Personal Information Protection and Electronic Documents Act (PIPEDA), Canada's new private sector privacy law, came partially into effect in 2001 and in 2004 will extend to all commercial activity in Canada except where provinces have passed substantially similar legislation.

Marleau reported that, in general, the introduction and implementation of the PIPEDA has gone far more smoothly than some had predicted. He noted that the business community has responded well to the demands of complying with the legislation, and that the new way of doing business has not on the whole been as difficult or traumatic as some had predicted. "We are seeing a general recognition that respecting privacy is not as onerous as some people thought and, in fact, is simply good business practice. One of the most encouraging signs is the obvious interest in compliance among the business community."

Marleau also reported that the ombudsman model has worked well with respect to the PIPEDA. Under the PIPEDA, the number of new complaints almost tripled over the last year, and Marleau expected a significant increase when the Act extends to all commercial activity in Canada in 2004.

For further information: www.privcom.gc.ca/information/ar/02_04_11_e.asp

UK businesses get guidance on e-privacy rules

The UK Information Commissioner's Office (ICO) has published guidance on the Privacy and Electronic Communications Regulations which enter into force on December 11th. The guidance spells out the steps businesses will need to take when marketing via e-mail and SMS, using online tracking technologies, and processing mobile location data.

The guidance helps to explain how businesses can meet the new 'consent' requirement for e-marketing, providing clarification on various marketing terms, such as 'unsolicited communications' and 'opt-in/opt-out'. Businesses will now be required to get 'opt-in' consent from consumers before sending them marketing material via e-mail or SMS. But, the ICO has confirmed that consumers will not necessarily have to actively tick a consent box and that businesses may be able to rely on less restrictive methods for obtaining consent. Its guidance states that to obtain consent, there "must be some form of communication whereby the individual knowingly consents."

The ICO has taken a lenient approach to the 'soft opt-in' exemption which allows businesses to avoid the higher opt-in/consent standard when marketing similar products and services to individuals whose data was collected in the course of a sale, or negotiations for a sale. The guidance states that an actual sale or negotiation does not necessarily have to take place. A consumer indicating an interest in purchasing a company's goods or services could also suffice.

The ICO even suggests that collecting data through competitions could fall under the soft opt-in exemption. Interestingly, however, the soft opt-in will not apply to charities and not-for-profit organisations. This contrasts an earlier position in which the ICO stated that the soft opt-in should also apply to the "promotion of aims and ideals". However, the ICO is to some extent hemmed in by the fact that the EU E-privacy Directive - on which the new regulations are based - states that the e-marketing rules apply only to commercial relationships.

Fortunately for businesses, the ICO has taken a pragmatic approach to legacy marketing data. Its guidance states that data collected before the December 11th deadline will not have to meet the opt-in consent standard, provided that the data was collected in accordance with the Data Protection Act and has been used recently. However, this looks is if it will only apply to e-mail as the ICO states that before the E-privacy Regulations were introduced, marketing via SMS or video messaging required consumers' prior consent.

The controls placed on e-marketing to corporate subscribers (eg. an e-mail address used for business purposes and paid for by an employee's company) are less rigorous. The guidance states that only "individual subscribers have an enforceable right of opt-out under these Regulations…This right does not extend to corporate subscribers." However, the ICO says that where marketing to corporate subscribers involves the processing of personal data (for example, an e-mail address contains the name of an individual), then the subscriber does have the right to opt-out.

The ICO's guidance has been published in two sections which are available via it website: www.dataprotection.gov.uk/dpr/dpdoc.nsf

On December 11th, PL&B hosts a conference in London taking an in-depth look at the new E-privacy regulations. For further information: www.privacylaws.com/whats-newframe.htm.

See p.18 for information on privacy and e-marketing across the European Union.

Australia publishes annual privacy report

Malcolm Crompton, the Federal Privacy Commissioner for Australia has published his annual report for 2002-03. According to the report, complaints to the Commissioner's office have risen over 70 per cent with 1,090 complaints made during 2002-03 compared to 632 in the previous year. 68 per cent of the total number of complaints were directed towards private sector organisations, with financial and telecoms companies attracting the lion's share of consumer grievances.

The most common cause of complaint was over the improper disclosure of personal data (28 per cent), with data security and quality both making up around 10 per cent of complaints. 18.5 per cent of the 651 complaints closed during 2002-03 resulted in a breach of the National Privacy Principles.

Because of the increase in complaints, the Commissioner announced that more staff resources have been directed at handling enquiries and complaints. However, he warned that this has affected the amount of resources that can be directed towards helping and advising the private sector. The annual report said that "focusing resources on responding to enquiries and complaints has substantially reduced the Office's capacity to engage actively with stakeholders...there have been many occasions where our advice has been sought in relation to emerging privacy issues in different industries, but we have been unable to assist."

A copy of the Commissioner's report can be found at: www.privacy.gov.au/publications/index.html#A

Job websites lack safeguards

A study published by the World Privacy Forum has found that online recruitment agencies are failing to implement robust privacy practices. The report claims that job sites are collecting excessive amounts of data that are not necessarily relevant to the recruitment process. One example highlighted in the report is Fast.web, a popular US search service for educational scholarships, which collects sensitive personal data such as sexual orientation and medical history.

The report also cites poor data accuracy, selling data to third parties, and a lack of transparency in online privacy policies. The report found that few sites had signed up to privacy seal programmes, while some were fraudulently displaying privacy seals.

For a copy of the report: www.pamdixon.com/wpfjobstudy.pdf

book review

European Privacy Laws

Baker & McKenzie, 2nd Edition, 2003
Price: € 50

Global law firm, Baker & McKenzie, recently published the second edition of its study into European data protection law. Since the first edition was published back in 1996, the data protection landscape across Europe has changed significantly with the majority of member states having now implemented the 1995 Data Protection Directive into national law.

However, although the intention of the directive was to harmonise regulation across the EU, every privacy practitioner operating in Europe knows there can be substantial and problematic differences between countries' interpretations of the directive.

For companies located across multiple European jurisdictions it is important understand what the local variations are, but this is not always easy considering the amount of legislation that exists and the lack of available comparative texts.

European Privacy Laws provides a overview of national privacy laws, allowing readers to compare and contrast the different interpretations across a wide range of issues such as consent, international data transfers, direct marketing, information notices, enforcement, and the use of data processors.

An example of the variations between EU laws is highlighted in the different approaches to handling consent for the processing of sensitive data. While the EU directive states that explicit consent is required, data protection authorities differ in their interpretation of exactly how organisations should go about obtaining this consent. In the UK, for example, there is a requirement to be "absolutely clear" and provide specific detail about the processing, while Italy requires consent to be submitted in writing or through the use of digital signatures. Spain similarly requires written consent, but makes an exception for the collection of medical data.

The book also reveals the mismatch of rules over direct marketing, with Germany and Italy requiring consumers to opt-in, while France, the Netherlands and the UK operate on an opt-out basis. These variations, however, should eventually be resolved through national implementation of the E-communications Privacy Directive.

European Privacy Laws examines a total of 21 countries, including the 15 EU member states and others such as Norway, Switzerland, Russia and the Czech Republic.

For further information, visit the publications section on Baker & McKenzie's website at: www.bakerinfo.com