INTERNATIONAL newsletter
ISSUE NO 65 NOVEMBER 2002

Editor & Publisher
Stewart H Dresner
stewart@privacylaws.com

Associate Editor
Eugene Oscapella
eugene@privacylaws.com

News Editor
Alan Pedersen
alan@privacylaws.com

Newsletter Subscriptions
Gill Ehrlich
gill@privacylaws.com

Issue 65 Contributors
Jeroen Terstegge
James Michael
Judith A Sullivan
Sandra Kelman

Contributions
Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items for consideration, contact: alan@privacylaws.com

Published by
Privacy Laws & Business,
5th Floor, Raebarn House,
100 Northolt Road,
Harrow, Middx HA2 0BX, UK
Tel: +44 (0)20 8423 1300
Fax: +44 (0)20 8423 4536
internet: www.privacylaws.com

Design by ProCreative +44 (0)20 8429 2400
Printed by Triumph Press +44 (0)20 8951 3883

ISSN 0953-6795

"privacy news"

Leading US drugstore in privacy probe

Walgreen Corporation has become the latest organisation to be embroiled in the Federal Trade Commission's (FTC) pharmaceutical marketing investigation. On October 17th, Walgreen, the largest drugstore chain in the US, revealed that the FTC had asked it for information relating to its privacy and marketing policies. A spokesperson for the company told *Reuters*: "We received a letter from the FTC asking for some information and we will provide that information and hopefully that will take care of their concerns."

Only a few days earlier, another drugstore giant, the Rite Aid Corporation, also revealed that it had been contacted by the FTC requesting documentation on its marketing practices. The FTC's actions signal an increasing concern that US drugstores are being paid by pharmaceutical companies to market products to their customers. Customers with a Prozac prescription, for example, could well find themselves being sent information relating to similar anti-depressant products that they have not requested. This practice does not necessarily mean that customers' information is being shared with the pharmaceutical companies. Walgreen, for example, has denied that it shares customer data with third parties. A spokesperson for Walgreen told *Reuters* that ""we do not provide any patient identifiable information to anyone outside the company."

Even though such organisations may not be sharing personal data with third parties, there is concern that customers are not being given proper or fair notice as to how their details will be used. Such was the case with the Eckerd Corporation, who settled with Florida's State Attorney General in July this year. Attorney General Bob Butterworth said that Eckerd did not "adequately inform" its customers that their details would be used for marketing purposes.

Reuters accused of corporate privacy invasion

Swedish IT firm, Intentia International, has filed criminal charges against *Reuters* after the news agency published allegedly private information about the company's earnings.

The information, which was contained in Intentia's third-quarter financial report, was published on their website and then accessed by *Reuters.* Although the web page was not secured or password protected, Intentia argue that because there were no hyperlinks directing visitors to the web page in question, it was therefore considered to be private information.

Commenting on the reports, *Reuters* denied that there was any substance to the allegations. Said Geert Linnebank, *Reuters'* Editor in Chief: "As one of the world's leading news organisations, *Reuters* is in the business of informing the market with breaking news stories using all the tools at its disposal, but doing so in a legitimate, ethical manner with journalistic integrity."

AOL ordered to reveal customer's identity

The US Supreme Court of Virginia has ruled that AOL must reveal the identity of a customer that has been accused of making libelous comments about Nam Tai Electronics. The electronics firm claims that the AOL customer, along with 50 others, posted the comments on an Internet message board.

AOL was served with a subpoena to reveal the customer's identity in January 2001, but the service provider subsequently made an appeal to quash the subpoena. Following the recent Virginia ruling, AOL has indicated that it may appeal the decision.

Further information:
www.computerworld.com/securitytopics/security/privacy/story/0,10801,75677,00.html

FCC seeks comments on telemarketing and privacy

The US Federal Communications Commission (FCC) has issued a notice of proposed rulemaking about possible revisions or additional rules relating to Congressional directives in the Telephone Consumer Protection Act of 1991 (TCPA). The TCPA regulates telemarketing and fax advertising.

The notice states that new technologies have emerged that allow telemarketers to better target potential customers and make it more cost effective to market using telephones and facsimile machines. According to the FCC, these new telemarketing techniques have also increased public concern about consumer privacy. It is asking for comment on whether to revise or clarify its rules governing unwanted telephone solicitations and the use of automatic dialing systems, pre-recorded or artificial voice messages, and facsimile machines.

Comments can be sent through the Commission's Electronic Filing System at: www.fcc.gov/e-file/ecfs.html. Comments are due by November 22nd 2002.

ISPs oppose UK data retention

Government plans to sign up UK Internet service providers (ISPs) to a voluntary data retention agreement have backfired according to recent reports. Under section 11 of the Anti-Terrorism Crime and Security Act (ATCS) 2001, the government was granted powers to create a code of practice governing the retention of customer data, including detailed logs of Internet and e-mail use.

The communications industry, however, has voiced concerns that the costs of retention will have a significant impact on its businesses. According to a regulatory impact assessment carried out by the government, the minimum costs were estimated at around £9 million (14 million euros) per year. Separate industry estimates have valued the cost at around £40 million (63 million euros) annually.

There has also been concern that excessive data retention could leave service providers in breach of the UK's Data Protection Act. A spokesperson for the Internet Service Providers' Association (ISPA) told *Reuters*: "We do not feel we can recommend Internet Service Providers voluntarily to comply with the government's proposed code of practice."

Although the ATCS code will be voluntary, it can be used as evidence in cases where a service provider has failed to retain data requested by law enforcement agencies. Should service providers fail to comply with the code, the government has powers to legally enforce it by introducing a statutory instrument before Parliament.

The EU has published a consultation paper on data retention.
See p.12 for more details.

CNIL approves student biometric ID project

The French data protection authority, the CNIL, has given the green light to a project that will allow the use of biometric technology to identify schoolchildren. The project will be carried out by the College Joliot-Curie, located in the town of Carqueiranne, and will require students to have their handprints scanned in order to gain access to the school's canteen services.

In 2002, the CNIL turned down a similar request from a college in Nice. In that particular case, the college wanted to use thumbprint verification technology to identify its students. The concern was that because thumbprints are a more commonly used identification technique, the school database could eventually be used for secondary purposes. The CNIL, however, has approved the use of handprint verification as a more privacy-friendly technology.

Korean regulators to monitor online privacy compliance

The Ministry of Information and Communication (MIC) is to carry out spot checks of around 300 e-businesses, according to a report in the *Korean Times*. Among the websites to be examined by the MIC are adult, chat room, and gambling sites. The sites will be checked for compliance with the national privacy law, which includes provisions on collection and use of data, and the privacy protection of children under the age of 14.

Meanwhile, according to Korean research firm, Nara, the number of unsolicited (spam) e-mails has risen 21 per cent in the last six months. The average number of spam e-mails received per day is now 10.2, from 9.3 in April. Among the types of mail cited, were advertisements for adult websites or bootlegged software and music.

Security and privacy to help Malaysian e-commerce growth

Reuters reported from Kuala Lumpur on optimistic predictions about the growth of e-commerce in Asia. Delegates to a recent ASEAN (Association of South East Asian Nations) Internet Trust Symposium heard the parliamentary secretary in Malaysia's communications and multimedia ministry suggest that growing familiarity with the Internet had helped offset initial fears about security when making payments online.

The report continues that Malaysia expects half of its seven million users to transact some form of business online this year, up from a third in 2001.

Further information: www.economictimes.indiatimes.com/cms.dll/articleshow?artid=26178181

EU publishes data protection reports

The EU's Article 29 Data Protection Working Party has published three new data protection reports. They cover:

- the party's opinion on the level of protection provided for personal data in Argentina
- the privacy implications of blacklists
- the transfer of airline passenger data to US government authorities.

The documents can be found at the

following address: www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm

United Arab Emirates needs privacy law says expert

Dr Zeinab Karake-Shalhoub, Associate Dean of the American University of Sharjah, has called for a new privacy law to help foster consumers' trust in e-commerce. Karake-Shalhoub told *Gulf News* that "many websites do not have a privacy statement. They are doing whatever they want to do." She added that the government has to "establish a framework by establishing rules and putting some teeth into it."

Canada: serious deficiencies found in control of federal ID numbers

Canadian businesses that rely on Canada's social insurance number (SIN) to prevent fraud at the hands of their customers will not be pleased with a recent government audit of the number's security.

The SIN is the federal government account number used to identify individuals for certain federal government purposes such as taxation, employment insurance and social benefit programmes. In a report released on October 8th, federal Auditor General Sheila Fraser found serious weaknesses in the control of the numbers. The number of usable SINs for people over 20 exceeded the actual population in that age group by 5 million. Among the Auditor General's other concerns:

• the identity and citizenship status of applicants were not checked adequately for the majority of SINs issued since 1998.

• inadequate control was maintained over SINs issued to people who are not Canadians or permanent residents. Although most of these people are expected to be in Canada temporarily, these SINs have no expiry date.

• despite an increase in its SIN-related fraud investigations, the federal department responsible for these investigations had not done a risk assessment to direct its efforts.

The Auditor-General noted the growing concern about identity fraud in both Canada and the United States, and that such fraud can be steps to far more serious crimes. She reported that the department responsible for issuing the SIN has recognised the problem and had taken some steps to address these issues "but it hasn't followed through".

Further information: www.oag-bvg.gc.ca/domino/reports.nsf/html/02menu_e.html

Payment card security scams leave consumers vulnerable

Credit card holders have long been warned to protect their personal information numbers (PINs) from curious onlookers when withdrawing money from automated teller machines. Now they have another worry – automated scams that bypass the security features of their debit cards.

According to police, the integrity of debit cards – cards used to purchase products by debiting the user's bank account directly at the time of the transaction – is being put at risk by a combination of technology and corrupt merchants.

Debit cards have a built-in security feature – the user's personal identification number (PIN) is needed to get access to the bank account associated with the card. *The Toronto Globe and Mail* reported on October 18th that some thieves now overcome this obstacle by using a "key catcher" to log PINs as customers punch them in. Thieves couple this key catcher with a point-of-sale computer which acts as a "skimmer" that takes down the card's magnetic strip data. Police suggest that this is a nearly undetectable way to steal the card PIN and the magnetic-strip data containing bank account information at the same time.

Armed with this information from corrupt merchants, criminals can create duplicate debit cards and use them to empty the victim's bank account. In Canada, petrol stations and convenience stores are the main sites for "skimming", according to police.

Major Internet computer servers attacked

The Associated Press reported on October 22nd an "unusually powerful electronic attack" that occurred the previous day and affected nine of the 13 computer servers that manage global Internet traffic. The source of the attack was unknown, and most Internet users would not even have noticed it. The attack worked by flooding the targeted servers with 30 to 40 times the normal amounts of data. *Reuters* news agency reported that the worst affected servers were in the United States, Sweden and Japan.

The FBI's National Infrastructure Protection Center is investigating.

Microsoft Outlook to block spyware

The upcoming version of Microsoft's mail client, Outlook, is to contain new privacy features that can stop marketers and spammers from deploying spyware such as cookies and web beacons onto users' hard drives. These technologies are traditionally used in HTML messaging, and can be used by spammers to verify active e-mail accounts when e-mails are opened, and whether users click onto any hyper-links in the e-mail. More importantly, Microsoft is to make the spyware blocking feature a default setting, so that uninitiated Internet users do not have to grapple with complex settings in order to protect their privacy.

Nokia launches mobile privacy solution

Nokia has released a new privacy solution for location-based services over mobile networks. The iGMLC Privacy Manager will allow network operators to provide location services to their customers while protecting their privacy. Consumers will be able to set their own privacy preferences and state where, when,

and by whom they can be contacted. "Operators have the responsibility to make sure that nobody misuses the location information of their customers," said Heikki Hemmi, General Manager, Location Business Programme, Nokia Networks.

California tops US privacy rankings

According to a recent survey published by the *Privacy Journal*, the state of California offers citzens the highest degree of privacy in the US. According to the survey, a raft of new privacy legislation over the last two years has helped to push California to the top of the pack, ahead of nearest rival, Minnesota, which came a close second. Both states have maintained strong privacy protection, far outstripping their competitors and ranking 33 per cent higher than third placed Connecticut.

The survey examined each US state according to a number of criteria including: the extent of privacy legislation; state enforcement of privacy rules; citizens rights to access and correct records containing their personal data; and rules limiting disclosure of personal information held by state agencies. The states were ranked into five tiers. Among the poorest performing states in the fifth tier were Texas, Kentucky, North Carolina, and Arkansas. Although federal privacy laws were not examined, Robert Ellis Smith, author of the survey and publisher of the *Privacy Journal*, said: "If the federal government had been ranked like a state, it would have [been] placed in the fourth tier."

P3P could lead to legal action

According to US law firm, Morrison & Foerster, websites that inaccurately implement privacy enhancing technologies (PETs) could face legal action from consumers.

The particular PET in question is P3P, a programme which automatically matches web users' privacy preferences against websites' privacy policies. However, it seems that the technology is yet to be developed to its full potential and may be giving web users a false sense of security. David Naylor, an e-commerce specialist at Morrison & Foerster, told the UK's *Financial Times* that P3P creates a "crude summary" of a website's full privacy policy which means that web users could be "getting a privacy policy that is inaccurate." According to Naylor, this inaccuracy could cause legal problems for website operators.

US financial privacy law is failing

By Eugene Oscapella

A recent Minnesota Law Review article by Edward J Janger and Paul M Schwarz, both of Brooklyn Law School, argues that the privacy provisions of the 1999 Gramm-Leach-Bliley Act (GLB Act) appear to have failed. The Act removed the legal barriers between different kinds of financial institutions. It allowed them to have closer business ties and create new kinds of "financial supermarkets". It also sought to introduce new rules for financial privacy, including notice requirements and opt-out provisions.

The authors describe four important aspects of the Act's privacy provisions. First, the Act requires the financial bodies it regulates to provide annual privacy notices that inform customers of their privacy practices. Second, it requires financial institutions to permit consumers to prevent their personal information from being shared with non-affiliated companies, which is achieved through an opt-out provision. Third, the Act requires financial institutions to develop policies to promote data security. Finally, it creates a right of enforcement, not for individuals, but for different federal agencies, including the Federal Trade Commission.

The authors conclude that the Act has disappointed both industry leaders and privacy advocates. In particular, they describe the failings of the opt-out requirement. Under the Act, financial institutions can disclose personal data to non-affiliated entities unless individuals take affirmative action by informing the institution that they refuse to share their personal information. The authors argue that this scheme is deficient: "By setting its default as an opt-out, the GLB Act fails to create any penalty on the party with superior knowledge, here the financial entity, should negotiations fail to occur. In other words, the GLB Act leaves the burden of bargaining on the less informed party, the individual consumer."

The authors argue that a notice and ""opt-in" regime might at first appear to be a better choice. Because consent must be procured, the burden shifts to the financial institution to convince a customer to permit disclosure. The institution must therefore explain the benefits of action. ""Opt-in creates an entitlement in the privacy of personal information, and the consumer must be induced to give it up."

Still, they conclude, even opt-in has its limits since it may well turn on unrealistic assumptions. "The manner in which banks, stockbrokers, and insurance companies use information, share information with affiliates and transfer information to third parties is complicated – too complicated to be understood by even a very smart lay person, let alone to be negotiated by each customer who opens a bank account."

Further information: E.J. Janger and P.M. Schwarz, "The Gramm-Leach-Bliley Act, Information Privacy and the Limits of Default Rules," 86 Minnesota Law Review 1219-61 (2002).