WORLD DATA PROTECTION REPORT

Volume 2, Issue 2 February 2002

Monthly news and analysis of data protection & privacy issues from around the World

HIGHLIGHTS

NEWS

CZECH LAW NOW PERMITS full communication with government authorities via the internet following the adoption by the Office for Personal Data Protection of a decree specifying the conditions for use of electronic signatures. (Page 3)

THE GERMAN GOVERNMENT is introducing a mandatory healthcare identification card to bring transparency and extra security to healthcare provision and billing, which would mean more protection for patients and help keep healthcare costs down. (Page 6)

JAPAN IS TO ENACT laws to combat spam mails sent to cell phones and personal computers. If parties fail to comply, the government will levy fines and stiff penalties. (Page 6)

U.K. LORD CHANCELLOR'S DEPARTMENT has published a summary of the responses to the public consultation exercise in relation to the Data Protection Act 1998. The government is deferring completion of its appraisal of the Act until the timing of the European Commission's report on the Data Protection Directive is clarified. (Page 8)

THE FEDERAL TRADE COMMISSION Bureau of Consumer Protection has announced a settlement of the dispute with Eli Lilly and Company for alleged violations of its online privacy policy. Although the settlement does not impose any monetary penalties on Lilly, it will be required to take appropriate measures to protect consumers' privacy in the future. (Page 12)

PRIVACY IN THE U.S. appears to be back on the agenda. Privacy advocates, lawmakers and some companies continue to argue that Congress needs to pass broader privacy legislation to address the increasing use of the Internet to collect personal information about privacy.(Page 14)

CASE REPORTS

COLOMBIA: A ruling by the Constitutional Court has provided greater clarity about the manner in which Internet websites should be registered with the authorities. The court set out the limitations on tax authorities concerning the information they may obtain about online transactions in Colombia. (Page 20)

UNITED STATES: The Supreme Court has refused to review a decision of the full Court of Appeals that a group of union-represented employees can proceed with invasion of privacy and emotional distress claims after they were secretly recorded in a workplace restroom. (Page 23)

COMMENTARY

ITALY: *Corrective Provisions on Data Protection*, by Alessandro del Ninno, of Studio Legale Tonucci, Rome. This article examines the important corrective and supplementary provisions with regard to the Italian Law of Privacy that came into force at the beginning of February 2002. (Page 25)

GERMANY: *Internet Data Protection to Become Easier*, by Dr. Kai von Lewinski and Dr. Marcus Schreibauer, of Lovells Boesebeck Droste. Collecting personal data is particularly important in the Internet industry. This article discusses the amendments made to the Teleservices Data Protection Act to make it more practical following representations from the Internet industry and data protection experts. (Page 30)

INTERNATIONAL DEVELOPMENTS

CYBERCRIME: As controversy continues to surround new cybercrime laws adopted around the globe, the Federal Government of Australia has approved a Cybercrime Act which expands the powers of government to carry out surveillance along Computer networks. The measures contained therein are similar to a Council of Europe Cybercrime Convention signed recently by 30 nations. The Treaty is being sent to individual states for ratification. (Page 32)

CONSUMER PROTECTION: Consumer and health protection authorities from 30 countries are to search thousands of websites in an effort to uncover deceptive, false or misleading health claims. The growth of the Internet has precipitated increased cross-border consumer transactions bringing law enforcement changes for authorities in each country. (Page 32)

In this Issue

AROUND THE WORLD

Australia: Bodies May Opt-in to National Privacy Principles . . . 3
Czech Republic: Decree on Electronic Signatures. 3
European Union: Standard Voluntary Contract to Ease EU Data Transfers . . . 4
Data Privacy Rules Meet EU Standards . . . 5
The Parliament Won't Eat "Cookies" . . . 5
France: M.P.s Grant New Internet Records Powers to Regulators . . . 5
Germany: Healthcare Identification Card to be Introduced for Population. . . . 6
Japan: Law Banning Spam E-Mails Planned . . . 6
United Kingdom: Government to Assess Compliance of U.K. Websites . . . 7
Data Privacy Law Abused, Resigning Commissioner Charges . . . 7
Data Protection Act 1988: Post-Implementation Appraisal . . . 8
Surveillance Law Unenforceable, Critic Charges . . . 11
United States: Unintentional E-Mail Disclosure Leads to Online Privacy Violation . . . 12
Privacy Outlook for 2002 . . . 14
"Don't Call" Registry Under Amendment to Telemarketing Rule . . . 16
Privacy Group Sues FBI to Release Purchase Records 16
Health Insurers Analyse State Privacy Laws . . . 17
U.S. Government Creating Computer Spy Viruses. . 17
More Security Problems Dog Microsoft . . . 18
Screening of Airline Passengers Raises Privacy Concerns . . . 18
Administration Stays on Sidelines of Privacy Debate 19

CASE REPORTS

Colombia: *Provision Imposing Obligations Upon Websites Declared Constitutional in Part Judgment C-1147 of 2001* . . . 20
Strasbourg: *Phone Taps in the Detection of Crime: PG and JH v. United Kingdom* . . . 20
United Kingdom: *When Public Interest Outweighs Protection of Press Confidentiality: Interbrew SA v. Financial Times and Others* . . . 22
United States: *Supreme Court Refused to Review Privacy Claims Decision: Consolidated Freightways Inc. v. Cramer, U.S. (No. 01-432)* . . . 23

COMMENTARY

Italy: Corrective Provisions on Data Protection . . . 25
Spain: New Electronic Signature Act Draft . . . 29
Germany: Internet Data Protection to Become Easier 30

INTERNATIONAL DEVELOPMENTS

Cybercrime New Cybercrime Plans for Australia Similar to Europe . . . 32
Consumer Protection Internet Sweep to Seek Cyber Health Scams . . . 32

WORLD DATA PROTECTION REPORT

WORLD DATA PROTECTION REPORT is published monthly by BNA International Inc., a subsidiary of The Bureau of National Affairs, Inc., Washington, D.C., U.S.A. Administrative headquarters: Heron House, 10 Dean Farrar Street London SW1H 0DX, England. Tel. (+44) (0)20-7559 4801; Fax (+44) (0)20-7222-5550; E-mail marketing@bnai.com. In the U.S. call toll-free on: 1-800-727-3116. Subscription price: U.S. and Canada U.S.$850/U.K. and rest of world £495. Additional copies of this publication are available to existing subscribers at half price when they are sent in the same envelope as a standard subscription. Reproduction of this publication by any means, including facsimile transmission, without the express permission of The Bureau of National Affairs, Inc. is prohibited except as follows: 1) Subscribers may reproduce, for local internal distribution only, the highlights, topical summary and table of contents pages unless those pages are sold separately; 2) Subscribers who have registered with the Copyright Clearance Center and who pay the $1.00 per page per copy fee may reproduce portions of this publication, but not entire issues. The Copyright Clearance Center is located at 222 Rosewood Drive., Danvers, Massachusetts (USA) 01923; tel. (508) 750-8400. Permission to reproduce BNA material otherwise may be obtained by calling (202) 452-4471; fax (202) 452-4084. Website: *www.bnai.com* *ISSN 1473-3579*

Editorial Director: **Joel Kolko** ***Development Manager:*** **Ashley Fillingham** ***Editor:*** **Eileen O'Grady** ***Production Manager:*** **Nitesh Vaghadia**

Correspondents: *Berlin:* David Graber; *London:* Patrick Tracey; *Paris:* Lawrence Speer; *Strasbourg:* Arthur Rogers

AROUND THE WORLD

AUSTRALIA

Bodies May Opt-in to National Privacy Principles

In a news release of January 10, 2002 the Australian Privacy Commission detailed the opting-in and opting-out provisions available under the Privacy Act.

It was pointed out that section 6EA of that Act allows small business operators, who would otherwise not be covered by the Act, to choose to be treated as an organisation for the purposes of the Act.

It was explained that this option had been made available in order to provide small businesses with the opportunity to benefit from any increase in consumer confidence and trust that may be derived from operating under the Act.

If a business decides to opt-in it will need to complete the Opt-in Application Form and return it to the Commission by mail. After verification, the name of the business and ABN (if it has one) will be placed on a public register as required by section 6EA(3) of the Act. There are no fees charged for opting-in.

If at any time and for any reason a business no longer wishes to be treated as an organisation for the purposes of the Act, it may opt-out by notifying the Privacy Commissioner in writing. Its details will then be removed from the register, and it will no longer be subject to the national privacy principles. No fees will be charged for opting-out.

The news release stated that it is important to note that any actions taken while the business is being treated as an organisation may be the subject of a complaint to the Commissioner, even if the business subsequently opts out.

Section 6EA(3) of the Privacy Act requires the Privacy Commissioner to record in a publicly available register all small business operators that have chosen under section 6EA(2) to be treated as an "organisation" for the purposes of the Act. The news release, accordingly, concludes with details of organisations which have made that choice. These appear, at the present time, to consist in the main of credit unions. See *www.privacy.gov.au*

CZECH REPUBLIC

Decree on Electronic Signatures

By Barbora Vinsova of Linklaters, Prague; E-mail: barbora.vinsova @linklaters.com. Reprinted from Linklaters & Alliance ITC Newsletter.

On October 3, 2001 the Office for Personal Data Protection (the "Office") adopted a Decree specifying the conditions for the use of electronic signatures (the "Decree"), which came into effect on October 10. Thus, Czech law now provides for the full implementation of e-signatures.

The Decree follows the Act on Electronic Signatures (the "Act") which came into effect in September 2000, and permits communication with government authorities via the Internet. Government authorities have started electronic registries for documents and this process should be finished by the end of the year.

The Decree specifies the cryptographic algorithms to be used when creating and verifying advanced electronic signatures. The main one is the RSA algorithm, which is commonly used worldwide.

Certificates

A certificate is a data statement issued by a certificate provider which links identity verification process. There are two kinds of certificates, ordinary and qualified. A qualified certificate is a certificate which satisfies all the conditions stipulated by the Act and the Decree.

Qualified certificates are provided on the basis of a written contract between a certificate provider and the electronic signature user. The Decree sets forth the requirements which devices used to create electronic signatures must meet in order to be considered secure for issuance of qualified certificates.

In the private sphere, e.g., for communication of banks with their clients or communication among companies, it is up to the parties to decide whether or not they will use qualified certificates, defined in the Act.

It is not possible to acquire a qualified certificate for the first time via the Internet without a personal visit to the certificate provider, as the latter must identify the applicant and store copies of his/her identity card.

Certificate Providers

There are three levels of certificate providers, namely "certificate providers", "qualified certificate providers" and "licensed certificate providers". Any provider can issue qualified certificates, but if it is not a licensed provider it must either notify the Office of such intention at least 30 days in advance or apply to the Office for accreditation and become a licensed certificate provider. Accreditation is subject to a fee of CZK 100,000. A licensed certificate provider generally must obtain the Office's consent if it wishes to conduct other business activities in addition to providing certificates; the only exceptions are that a licensed certificate provider may also be, if separately qualified, an attorney ("advokat"), notary, or registered expert.

Only advanced electronic signatures and public keys issued by licensed certificate providers can be used in dealing with public authorities.

Any person authorised to conduct business activities in the Czech Republic can qualify as a Czech provider of qualified certificates. Foreign entities can conduct busi-

ness activities in the Czech Republic only through a registered branch office (or, of course, by establishing a Czech subsidiary).

Security of Electronic Signatures

Technical Aspects

Electronic signatures are based on asymmetric cryptography, using two separate keys, a "private key" and a "public key", to encrypt and decrypt messages. Each pair of keys must be generated together. The signature is created by combining a sender's private key and a message digest (the document, electronically reduced by "hashing"). The recipient then uses the sender's public key and the message digest to verify the sender's identity and integrity of the document.

The operation is executed in only one direction, i.e., the sender always uses only his/her private key and the recipient always uses only the sender's public key. However, the possibility that the sender's private key could be broken by an unauthorised person cannot be ruled out, although this would require computing capacity that is normally unavailable. Thus, for security reasons it is recommended to change the pair of keys on a regular basis, e.g. every three months, depending on how often the electronic signature is used. The longer the keys are the more difficult it is to break them. The data which is used to create an electronic signature needs to be kept in a safe place, as with protection of credit cards and PIN codes.

Legal Aspects

The mechanism of advanced electronic signatures makes it possible to reliably identify the user, and the electronic signature is legally binding. If a user becomes concerned that his/her electronic signature is no longer absolutely secure he/she can ask the certificate provider to put his/her qualified certificate on the Certificate Revocation List, which serves as notice that the signature is no longer used by the correct party. The Decree specifies that the Certificate Revocation List must be accessible by two independent methods that ensure long-distance access.

The recipient of a message with an electronic signature should check the Certificate Revocation List to see that the sender's public key has not been revoked. From this point of view the protection offered to the message recipient is higher than in the case of a manual signature, since he/she takes an active part in the verification process. If a certificate provider fails to register the revocation of a certificate it is liable under the Civil Code for the damage caused to the parties.

EUROPEAN UNION

Standard Voluntary Contract to Ease EU Data Transfers

BRUSSELS—The European Commission adopted a standard voluntary contract that can be used to facilitate personal data transfers to third countries that lack laws providing "adequate protection" based on European Union data privacy standards.

Under the standard contractual clauses, an EU company exporting data should instruct its subcontractor to treat the data with full respect for EU data protection requirements and should guarantee that appropriate technical and security measures are in place in the destination country.

> "This is an additional practical measure making it easier for companies and organisations to comply with their obligation to ensure adequate protection for personal data transferred from the EU to the rest of the world while safeguarding individuals' right to privacy," said EU Internal Market Commissioner Frits Bolkestein.

The standard contractual clauses are not compulsory for businesses.

> "The advantage of using these standard clauses when transferring personal data or processors in countries outside the EU is that member states' data protection authorities are obliged to recognise that these transfers enjoy adequate protection," said Commission spokesman Jonathan Todd.
>
> "The standard contractual clauses therefore add a new possibility to those already existing under the EU Data Protection Directive, which establishes several cases where data may still be transferred to countries where the data protection regime is not adequate.
>
> "These include cases where individuals have given their unambiguous consent for data to be transferred outside the EU and where the transfer is necessary for the conclusion or performance of a contract in the interest of the data subjects," Todd added. "In addition, member states' data protection authorities may authorise such transfers on a case by case basis when they are satisfied that the processing in a non-EU country enjoys adequate protection."

American companies that comply with the Safe Harbor Privacy Principles do not need to use the standard data privacy contract issued by the EU.

The standard contract complements other clauses approved by the Commission in 2001 that establish standard clauses for the transfer of personal data to controllers. That decision (EEC/2001/497) spells out the rights and obligations of the so-called "data controller" in the EU and the "data processor" established in a non-EU country. These provide guarantees for a subcontractor processing data on behalf of a data controller and the necessary safeguards that both need to fulfil in order to be able to carry out the processing of personal data outside the EU.

For more information about the new standard contract clause, consult the following Internet website: *www.europa.eu.int/comm/privacy.*

EUROPEAN UNION

Data Privacy Rules Meet EU Standards

BRUSSELS—New Canadian data privacy rules have been deemed "adequate" to meet European Union standards designed to protect information about European individuals when it is transferred across the Canadian border, the European Commission announced on January 14, 2002. The Commission also said it based its decision on the contents of the Canadian Personal Information Protection and Electronic Documents Act.

The Canadian law entered into force on January 1, 2001, and applies to personal information about clients and employees of federally regulated organisations such as airlines, railways, shipping, inter-provincial trucking, banks, television, radio, television and telegraph collected, used and disclosed in the course of a commercial activity, the commission said. The law also applies to all organisations that disclose personal information for consideration outside a province or outside Canada.

As of January 1, 2002, the Canadian law has applied to health information held by federally regulated organisations. By 2004, the Canadian law will cover every organisation that collects, uses and discloses personal information in the course of a commercial activity whether or not it is federally regulated.

The EU-Canada data privacy agreement does not cover personal data held by public institutions at the federal and provincial level or personal data held by private organisations and used for non-commercial purposes such as data handled by charities or collected in the context of an employment relationship.

> "For these transfers to recipients in Canada, operators in the EU will have to put in place additional safeguards such as the standard contractual clauses adopted by the commission in June of 2001 before exporting data," the commission said.

Canada joins Hungary, Switzerland and the United States as the only countries that have been approved by the European Commission as having data privacy protection standards that meet EU standards.

The EU Data Protection Directive agreed in 1995 requires that any country where data is being imported about EU citizens must have measures similar or "adequate" to those in the 15 member states.

EUROPEAN UNION

The Parliament Won't Eat "Cookies"

Extracted from "the l.i.n.k." (a free bi-monthly electronic newsletter on Information Society legal issues, edited by Le_Goueff@vocats.com)

The 26th amendment proposed by the Parliament with respect to the proposal for a European Parliament and Council directive concerning the processing of personal data and the protection of privacy in the electronic communications sector (COM(2000) 385) intends to add to article 5 of the Commission initial proposal a paragraph 2a, providing that:

> "Member states shall prohibit the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user without the prior, explicit consent of the subscriber or user concerned. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network".

This text is directly connected to the famous "cookies", those little files saved on the user's computer in order to provide him with more personalised services.

The Parliament wants member states to require the explicit consent of the recipient of a cookie before it can be sent, providing that this will ensure non-abusive use of the collected data and thus protect privacy.

The full text of the Commission initial proposal can be downloaded (.pdf format) at: *http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/documents/com2000-385en.pdf*

The Parliament's proposed amendments can be found at: *http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/index_en.htm*

For more information contact: le_goueff@vocats.com

FRANCE

M.P.s Grant New Internet Records Powers to Regulator

PARIS—The French National Assembly adopted on December 20, 2001 an emergency amendment to the 2002 Budget Bill offering customs officials, tax collectors and securities regulators new powers to review and retain data from Internet Service Providers (ISPs) in the course of investigations of civil or criminal wrongdoing.

The amendment will give regulatory authorities many of the same investigative powers already granted to judicial and law enforcement agencies in late October, when the National Assembly obliged ISPs to conserve connection data and user logs for one year and make records available to police and judicial officials upon request as part of omnibus anti-terrorism legislation.

Civil liberties advocates and privacy experts have sharply attacked sections of the Law on Daily Security (No. 718-01), which allows the government extended powers to eavesdrop in cyberspace and obtain and keep ISP records for use in investigations. Similarly, privacy advocates are demanding greater counter-balances to the new interception rights granted to tax, customs and securities regulators.

French government officials are now preparing an administrative decree, in cooperation with the national privacy watchdog CNIL, which will lay out the nuts-and-bolts of how the one-year data conservation rule will be applied and the exact circumstances under which judicial, law enforcement and regulatory officials can seize ISP data.

GERMANY

Healthcare Identification Card To be Introduced for Population

BERLIN—The German government plans to introduce a mandatory healthcare identification card, Minister of Health Ulla Schmidt announced on December 3, 2001.

Schmidt said that her ministry would test the idea this year in regional pilot projects to examine the usefulness of such a card for individual treatments and controlling costs.

The universal card is an expansion of Schmidt's plan to create a card for tracking users of certain medicines, announced on August 23. The minister proposed the card, as part of a quick-alert system for patients and health professionals, in the wake of allegations that use of Lipobay, a fat-reduction product of Bayer AG, had resulted 52 deaths worldwide.

The computer chip on the card would give doctors and pharmacists immediate access to a patient's health status and medications. The ministry said that the card would also bring transparency and extra security to healthcare provision and billing, which would mean more protection for patients, and help keep healthcare costs down.

To Link Existing Records

The ministry said it had established a project group which is designing the card based on patient medical documentation records, and setting up a system for linking patient files and data banks. Implementation of the card would include an electronic process for writing and filling prescriptions, which would make use of already existing databases on individual patient allergies to certain medicines.

The ministry said that data protection concerns would play an important role in designing the card, and that the patient would retain control over the data and be able to decide who would have access to it. The cards will not create so-called "glass patients", according to Schmidt.

The minister said that many hospitalisations occur because patients receive treatments from various sources, and one prescribing doctor may not be aware that the patient is already taking other medicines under another doctor's care—because there is no one common file kept on the patient, the minister said. The healthcare identification card would document and allow for coordination of all treatments, and would, for example, give doctors an automatic procedure for checking for allergies to certain kinds of medicine. This could also help avoid unnecessary repeat examinations or parallel treatments.

The ministry said the universal card would improve the safeness of medical treatments because the card would ensure that information on innovations in medicine or possible effects of combining drugs could be sent directly to patients' caregivers and pharmacists. Also, the card ought to help optimise work processes, and encourage patients to take more self-initiative and individual responsibility.

Officials Against Requiring Card

Germany's Federal and State Data Protection Commissioners said on December 4, 2001 that they did not support the idea of making the card compulsory and warned the government against the idea. The officials said that they did not fundamentally oppose a universal healthcare identification card, but that the government should guarantee that use of the card would be voluntary.

The commissioners justified their position by noting that one of the most basic rights of patients is to decide for themselves to whom and to what extent to reveal personal information. This right could be stripped of substance if, in addition to the card, the government established an obligation to present the card to healthcare professionals. Patients may not wish to reveal their entire medical history to every doctor or pharmacist they consult, for example. Also, having the patient's entire treatment history available on the card could interfere with the practice of seeking to obtain an unbiased second opinion.

Putting all current health and illness records into a central medical databank would create a file with information on 90 percent of all people in Germany, which presents an enormous risk for potential misuse of the data, the commissioners said. Additionally, the idea of a introducing a call-centre for giving out patients' medical data raises reliability concerns.

JAPAN

Law Banning Spam E-Mails Planned

TOKYO—Japan is moving to enact laws for combating spam mails sent to cell phones and personal computers, including the ban on spam transmitters and stiff penalties on parties that violate the laws.

The plan is being considered by Prime Minister Junichiro Koizumi's Liberal Democratic Party (LDP) and its two coalition parties, as well as by the Ministry of Economy, Trade and Industry (METI). The lawmakers hope to draft legislation for a new law and/or amendments to existing laws for submission to the next regular Diet session by Spring 2002, an LDP secretariat official said.

The lawmakers plan to require that parties that transmit e-mails in a broadcasting fashion enter their names, physical addresses, mail addresses, and explanations that

their e-mails and transmission conform to relevant laws. Transmitting parties can be corporations, individuals, non-profit organisations, public corporations and others living in Japan and overseas.

When transmitting parties continue sending spam despite the refusal of parties receiving e-mails, the new law and/or amendments would empower the Japanese government to order the transmitting parties to discontinue doing so, and if they fail to comply the government will levy fines and stiff penalties, the official said.

METI is considering a less stringent measure because of concerns that imposing strong regulations might hamper the growth of information and telecommunications development. It is recommending amending the Specific Commercial Transaction Law and punishing violators with up to two years' imprisonment or a three million yen ($25.000) fine.

The Tokyo municipal government is considering tracking down spam transmitters and punishing them with the city's ordinances, a city spokesman said.

According to a spokesman for NTT DoCoMo, the mobile telecom subsidiary of Nippon Telegraph & Telephone Corp., its cellular communication control centre receives approximately 950 million e-mails everyday of which 800 million are undeliverable, suggesting they are spam mails.

Before legislative action, METI will require that all e-mail advertisements carry the message "advertisement!" in Japanese, effective from February 1, 2002, a METI official said. Exceptions are ads that consumers requested for transmission directly to advertisers. In addition, METI will require that e-mail ads state methods of contact and physical contact addresses, he said.

UNITED KINGDOM

Government to Assess Compliance of U.K. Websites

The U.K. Information Commissioner's office will evaluate the data protection compliance at various websites. The aim of the project is to assess the sites' compliance with the Data Protection Act and the Freedom of Information Act, and to generate awareness among U.K. site operators of their legal obligations. The project will involve about 130 U.K. websites and should be completed by May 2002, said Ian Bourne, the government agency manager in charge of the project.

> "There are a number of aspects to the research. The plan is for the researchers to look at those websites they can identify as being U.K.-based and assess their compliance with data protection legislation," Bourne said.

Although there have been previous surveys into U.K. website compliance with data protection legislation, they were conducted by commercial interests.

> "We're planning to go beyond simply checking for a 'glossy data protection statement' on a website," he said. "To do this, researchers will use telephone and face-to-face interviews, backing up their interviews with mystery shopper techniques, rather than take what the sites say at face value."

Tarlo Lyons, a London-based law firm specialising in information technology, has given a cautious thumbs-up to the project, saying all British websites should have complied with the Data Protection Act by October 24, 2001.

The Information Commissioner's website is available at: *www.dataprotection.gov.uk*.

UNITED KINGDOM

U.K. Data Privacy Law Abused, Resigning Commissioner Charges

LONDON—Government ministers have failed to protect the public from abuse of data privacy laws by undermining the role of the information watchdog, a report to government from the U.K. Data Protection Agency said on January 9, 2002.

Information Commissioner Elizabeth France, who heads the Data Protection Agency, said that in 2001 alone the Information Commissioner carried out a record 8,000 investigations into alleged breaches of the 1998 Data Protection Act, mostly involving organisations wrongly disclosing confidential data to third parties.

She accused government ministers of undermining her role as Information Commissioner and ignoring her calls for criminal penalties against violators. The government had "hindered the protection of the public," she said.

France accused the government of sacrificing "better regulation for minimum regulation" and said that unnecessary restrictions on the Data Protection Agency were "inconsistent" with data protection duties under European law.

The commissioner, who will step down from her job in November 2002, said she wanted her successor to be granted powers to bring criminal prosecutions against those who breach the law. France has consistently criticised the government's "cult of secrecy" during her seven years as Information Commissioner.

The report highlighted Internet trading as one of the most egregious areas of illegal disclosure of personal financial details.

> "There have been several instances of inadequate security as a result of which the personal details of customers have been disclosed on a website," the report said. "If the data controller has wilfully or negligently failed to secure the website but does so following the breach, there is no penalty the commissioner can impose."

Complaints Cited in the Report

The report cited a recent complaint to the commission over police records sent to a Bristol University and later found on a computer sold to a member of the public. The files named 11 alleged paedophiles and their victims. The report said that the victims and their families were unaware that the details were released to the university by police. A Bristol University spokesman said the information, including testimonies and transcripts of police interviews, was transferred to the university's law school for a study into how evidence was gathered in cases of child abuse.

In another complaint received by the commissioner, school pupils who were given holiday work experience at their local authority offices were privy to their teachers' employment records.

The Data Protection Act 1998 came into force almost two years ago. France's report was part of an appraisal of the impact of the law and will be forwarded to the European Commission for its own report on the implementation of the EC Data Protection Directive.

> "There is much that the commissioner welcomes in the new law ... but this submission necessarily concentrates on what she sees as the deficiencies," the report said.

Commissioner Stepping Down

France also announced that she would be stepping down from her post. Her resignation, effective when her contract expires in November, followed a dispute with Home Secretary David Blunkett over provisions in the Anti-Terrorism, Crime and Security Bill that allows the retention of communications data by public communications providers for later access by law enforcement agencies.

France expressed concerns during the month of December 2001 about the government's steps to monitor personal emails. But the Data Protection Agency denied that France's regulation was related to this recent dispute. "It is the end of her term of office, and the post has to be advertised anyway," said Pat Mellor, France's personal assistant.

For More Information: The Information Commissioner's "Guide to Data Protection Auditing" is available at on the agency's website at: *www.dataprotection.gov.uk/dpaudit*.

UNITED KINGDOM

Data Protection Act 1998: Post-Implementation Appraisal

Introduction

In September 2000, some 6 months after the Data Protection Act 1998 came into force, the Home Office carried out a public consultation exercise to help it make an early appraisal of the Act's impact. Work on the appraisal had not been completed when responsibility for data protection was transferred from the Home Office to the Lord Chancellor's Department under the post-election machinery of Government changes. As the appraisal questionnaire explained, part of the purpose of the appraisal was to inform the United Kingdom's approach to the European Commission's first report on the implementation of the EC Data Protection Directive, which was due in October 2001.

The Commission's report has been delayed. Until the timing of the Commission's report is clearer, the Government is deferring completion of the appraisal of the 1998 Act. This will allow any additional lessons learned from the continuing experience with the 1998 Act, as well as any other relevant developments, to be taken into account. The Government thinks it would be helpful, however, to make available now a summary of the responses to the consultation exercise. There were about 100 responses including a detailed paper from the Data Protection Commissioner (who has since become the Information Commissioner and is subsequently referred to by that name in this paper).

Part A of this paper contains a brief summary of the main points raised in the responses other than that of the Commissioner. Part B summarises the comments made by the Commissioner. Her comments are summarised separately because of her unique position as the supervisory authority for the 1998 Act. A list of all the respondents who offered comments is attached at the Annex.

If you require further information about the responses to the consultation exercise, please contact: Paul Henery, Freedom of Information and Data Protection Division, Lord Chancellor's Department, 50 Queen Anne's Gate, London SW1H 9AT. E-mail: paul.henery @homeoffice.gsi.gov.uk; Tel: 020 7273 3723; Fax: 020 7273 2684

Comments of Respondents Other Than Information Commissioner

Scope and Definitions

(a) Is it clear what manual records are caught?

Some respondents had problems understanding what constituted a "relevant filing system" and felt that further guidance was needed.

(b) Is the definition of "personal data" clear?

Some respondents had difficulty with the definition. For example, how could controllers tell whether identifying particulars were "likely to come into" their possession? There was a suggestion that personal data protected during a person's life should not lose that protection immediately upon the person's death. It was also suggested that, like the Data Protection Act 1984, the Act should apply only to data processed "by reference to the data subject".

(c) Is the relationship between the "data controller" and the "data processor" clear?

Some respondents felt that the relationship was unclear, particularly where an organisation was large and complex, such as the National Health Service, or where

complex financial and legal relationships exist, such as in the insurance sector. Other areas of difficulty included the relationship between the Crown Prosecution Service and counsel, and that between a pupil master and his pupil.

Data Protection Principles

(a) Are the conditions for processing clear and useful?

There were concerns about the interpretation of a number of the terms used, in particular "consent". Definitions of "consent" and "explicit consent" would be welcome. A number of respondents were uncertain when a condition other than consent, can be relied upon. Some also saw a problem when consent has to be given on behalf of another person, for example, a minor. Some respondents thought that the conditions were unnecessarily wide. A specific example related to health records where it was suggested that confidentiality and the interests of patients were not best served by the width of the conditions.

(b) Is it clear that satisfying the conditions does not discharge the requirement to comply with the Principles?

The majority of respondents realised that this was the case. However, it was suggested that clarity would be improved if the First Principle requirements to process fairly and to process lawfully were separated.

(c) Is it clear what information has to be provided to data subjects and when?

(d) Are there any practical difficulties with the provision of information?

Definitional problems were raised by a number of respondents: clarification was sought on the meaning of "relevant time", "disproportionate effort", "at that time" (Schedule. 1, Part II, para. 2(2)(b)) and "any further information" (Schedule. 1, Part II, para. 2(3)(d)).

A number of the responses were concerned with procedural matters such as the correct course of action in particular situations. One respondent suggested that there should be a Code of Practice covering this area.

A number of respondents felt that there were real practical problems in meeting some of the obligations imposed by the Act. It was felt that compliance was impracticable when there was a large volume of data and the relationship with the data subject was remote. Even relatively hands-on relationships caused problems. Examples were out-patients and emergency cases in the NHS.

There was concern over the economic impact of the provision of information. As well as the cost of providing the information, the provision of the information on the telephone when selling a service or product measurably resulted in abandoned calls and lost sales; and it was difficult to incorporate the information into written material (e.g. for charitable appeals) in a way which was not off-putting.

Sensitive data

(a) Are the categories of sensitive data appropriate?

Some respondents suggested additions to the "sensitive data" category (e.g. sensitive occupations, digital signatures and financial information). There was a suggestion that trade union membership should be removed.

Problems of interpretation included:

- whether surnames indicate race;
- whether a purchase order (e.g. for kosher food could indicate race);
- whether processing of personal data by a church indicates religious belief.

(b) Are the conditions for processing sensitive data appropriate?

There was some concern among respondents that the conditions restricted necessary processing. For example, there is an impediment to processing for insurance purposes involving several people (e.g. group travel insurance), since the explicit consent of all the data subjects is needed. It was also unclear whether the processing of data on ethnic origin for the purposes of equal opportunity monitoring is permitted. A case was seen for resolving some of the difficulties through subordinate legislation.

There was a suggestion that a problem arises when information is spontaneously provided by the data subject. It was felt that the fact that the data subject had provided them should be a sufficient ground for processing the data (i.e. there should be no need to seek "explicit" consent).

Data Subjects' Rights

(a) Are the rights of data subjects sufficiently clear?

The majority of respondents felt that the rights of data subjects were sufficiently clear. Some controllers were concerned about being swamped by subject access requests. However, other respondents thought that the rights were not sufficiently publicised. Clarification was sought of certain terms and concepts:

- "reasonable" (s. 7(4) - (6));
- "unwarranted substantial damage or substantial distress" (s. 10(1)); and
- the scope of the right to prevent direct marketing.

Some extension of existing rights was suggested. For example, data subjects should be entitled to be informed of their right to object to fully automated decisions being made about them. There should be a right to compensation where breaches of the Act result in distress.

(b) Are the revised arrangements for subject access satisfactory?

There was concern about the level of the subject access fee. Some respondents felt that the present fee was too low compared to what was often a large amount of work involved in providing access. There was particular concern about the arrangements in the health sector. Some felt the £50 maximum for access to manual health records disadvantaged data subjects. Others were concerned about the possible reduction to £10 from October 2001. [NOTE: An order has been made retaining the fee at £50 for the time being. The Government will work with the Information Commissioner, in consultation with other key interests, with the aim of finding a long-term solution.]

(c) Is the scope of the exemptions from subject access satisfactory?

Suggestions were made for clarification and/or extension of the present arrangements for:

- the definition of "likely to prejudice" in s. 29(1);
- the national security exemption;
- the position in relation to references given and received;
- fraud prevention;
- lawful investigations;
- information provided in confidence;
- back up and audit data;
- commercially confidential information.

Notification

(a) Are there any problems with the categories of information to be notified to the Commissioner?

Most respondents felt that there were no significant problems.

(b) Do the procedural arrangements as provided for in the legislation work?

Again, respondents were generally content, but one suggestion was that the notification period (one year) should be the same as the previous registration period (three years). One respondent suggested that notification did not contribute to the protection of personal data.

(c) Is it useful to have the exemptions?

The majority of respondents approved of the exemptions. Concern was expressed about whether small sports clubs were exempt; and that barristers were not.

(d) Is it easy to decide whether you benefit from an exemption?

While both the information about exemptions on the Information Commissioner's website and in the notification handbook issued by the Commissioner were thought to be helpful, some respondents still felt that there was a lack of clarity.

(e) Do the standard purposes cover all routine processing?

The majority of respondents were content that all routine processing was covered, but it was suggested that "research" should be added.

International transfers

(a) Has the rule in relation to international transfers restricted your transfer of personal data outside the EEA, including via the Internet?

It was felt by some respondents that the rules in this area were not easily understandable and that problems were likely to increase with the growth of e-business. However, the "safe harbour" agreement with the U.S.A. was welcomed. It was suggested that a model contract for data exports should be available on a website. [NOTE: Information about the European Commission's work on standard contractual clauses for data exports is available]

(b) Do you find assessing adequacy difficult?

It was suggested that there was a need for guidance on the assessment of adequacy. Against this, there was a view that controllers should not be circumscribed in making decisions about adequacy.

(c) Are the exemptions clear and useful?

Most respondents found the exemptions to be clear and useful.

Compliance

Are the Commissioner's powers appropriate?

Most respondents who commented on this question felt that the Commissioner should have stronger powers (and more resources). A number of the specific suggestions related to her powers to conduct assessments. One respondent suggested that the Commissioner's powers to issue Codes of Practice diminished controllers' freedom to interpret the legislation.

New Technology

(a) With the exception of international transfers, have you found difficulties in meeting the Act's requirements when using the Internet?

(b) What changes are needed to make compliance easier?

The main concern expressed by respondents in this area related to the speed with which technology may have overtaken the provisions of the Act. This was reflected in a number of practical problems being highlighted with regard to encryption and security, and the way in which sensitive information can be routinely processed on the Internet.

Other comments

Other points made included:

- concern about the inherent complexity of the Act;
- a request for clarification of what constitutes processing for "personal, family or household purposes";
- a suggestion that the Act restricts the flow of information to the media;
- concern about the wide scope of the exemption for processing for "special purposes";
- concern that the Act fails to take account of the way in which the very large number of small voluntary organisations work;
- concern about possible conflict with the Human Rights Act;
- concern about differential implementation of the Directive within the EU;
- a suggestion that the Act should not apply to "transient" data generated while a document is being word processed if the Act would not apply when the document is subsequently stored.

Comments of the Information Commissioner

Since the specific questions asked by the Home Office appear to be directed primarily to data controllers, the Commissioner's response follows a different format. It looks first at the Directive, then at the form of the U.K. law implementing the Directive, and finally at some specific problems with the 1998 Act. The Commissioner makes clear that there is much that she welcomes in the new law.

The Directive

The Directive does not always protect privacy in the most effective or efficient way. The Commissioner favours a simpler, more flexible and less prescriptive instrument.

Article 4: The extra-territorial provision is hard to justify and makes little sense.

Article 8: The concept of "sensitive data" is misguided. Sensitivity depends on context. It is best addressed by appropriate interpretation of the data protection principles. The conditions for processing sensitive data do not achieve their aim.

Article 11: The provision made as to the time at which information must be given to individuals is flawed.

Article 15: The justification for this Article is unclear.

Article 17: The requirement for there always to be a written contract when a controller uses a processor is overly prescriptive.

Article 18: The notification provisions impose burdens which are disproportionate to any benefits. If retained, they should be limited to the provision of details about controllers and the nature of their business.

Article 25: The requirement for "adequate" protection in third countries is sound, but the provisions relating to trans-border data flows are over-prescriptive and place undue emphasis on centralised decision-making.

Implementation in the U.K.

The 1998 Act could have been less complex and less burdensome for business while providing individuals with simpler, more effective rights.

Section 13: Compensation should be available for contraventions of the Act which cause distress even if there is no damage.

Section 22: No "assessable processing" should be designated.

Section 23: The Government should keep open the possibility of an order providing for the appointment of data protection supervisors.

Section 32: The exemption for freedom of expression is particularly difficult to understand.

Section 34: The exemption for information required to be published is very wide and has no obvious basis in the Directive.

Section 42: The Commissioner should have discretion whether or not to carry out an assessment.

Section 51: The Commissioner should be empowered to carry out data protection "audits" without the consent of the data controller.

Section 59: The restrictions (backed by a criminal penalty) on the disclosure of information imposed on the Commissioner are disproportionate.

Section 60: It should be an offence for data controllers knowingly or recklessly to breach the data protection principles to a significant degree.

Schedule 1: The first data protection principle should be restructured to make its different elements clearer.

Schedule 3: Additional "gateways" for the processing of sensitive data without explicit consent are needed. This is a priority for the Commissioner.

Data Protection Act 1998

Section 1: Inconsistencies between some definitions in the Act and those in the Directive cause lack of clarity. The definition of "relevant filing system" is a particular problem.

Section 7: There should be a consistent approach to subject access fees.

Section 12: The terminology used is, unhelpfully, different from that in the Directive.

Section 16: Allowing controllers to choose whether or not to include details of their processing which is exempt from notification is unhelpful. There should be a simple statement pre-entered in every register entry to cover this.

Section 36: The exemption for domestic purposes should be limited to processing which does not prejudice the rights and freedoms or legitimate interests of others.

Section 53: The Commissioner's power to assist individuals in proceedings under the Act should not be limited to "special purposes" cases.

Section 56: The Commissioner may, when she has further evidence, wish to seek an extension of the scope of the prohibition of enforced subject access to cover health records.

Section 57: This provision seems redundant.

Schedule 1, Part II, Paragraph 3: The conditions set out in the Data Protection (Conditions under Paragraph 3 of Part II of Schedule 1) Order 2000 are cumbersome and onerous.

UNITED KINGDOM

Surveillance Law Unenforceable, Critic Charges

LONDON—Internet surveillance laws in the United Kingdom that will require service providers to retain data and information about users could violate the European Human Rights Act, the Foundation for Information Policy Research said on January 18, 2002.

Caspar Bowden, who heads the foundation, said the Regulation of Investigatory Powers Act (RIPA), which came into force last year, is "unenforceable. Blanket traffic retention is a breach of the Human Rights Act." He said:

> "All the data protection heads across Europe have been saying this for two years. They are the legal authority and the government is ignoring what they say."

Bowden singled out for criticism a plan he said would force Internet service providers to install devices to monitor Internet traffic. He said the an amendment, known as the Technical Advisory Board Order, would

require service providers to install so-called "black boxes" similar to those used as flight recorders. The order was rushed through Parliament in October 2001 despite demands from industry and civil libertarians for more time to study the details, he said.

Bowden claimed that the reason the order was fast-tracked through Parliament had little to do with investigating terrorism in response to the September 11 terrorist attacks upon the United States.

> "The data can be obtained for public order offences, minor crimes and tax evasion," he charged. "The fact that very little on the statute book is usable may be a victory for civil liberties campaigners, but if the legal principle is accepted today it is still a tragic loss of civil liberties."

He said the order threatens the privacy and civil liberties by allowing any public servant nominated by the Home Secretary to order the collection and retention of any emails or phone calls sent or received. The information could be given to the FBI or law enforcement authorities in the European Union, he said.

> "The law has been exposed as unworkable, and has ended up bungled. In the end, everyone—both civil liberties campaigners and the law enforcers—has lost," said Bowden.

However, the Home Office insisted that the communications data provisions are not a "backdoor" means of accessing communication content. Whereas communications data had previously been sought under a variety of powers, RIPA "simply places these arrangements on a statutory basis, and [the order] tightens them considerably," a Home Office spokeswoman said.

The law "does not require service providers to install a 'black box' which will monitor all Internet traffic," said Home Office spokeswoman Gemmaine Walsh. "This allegation is completely false," she said. "The law does not ask for it, and reports of 'black boxes' by the press are confused and inaccurate."

She acknowledged, however, that clause 12 of the Act enables the Home Secretary to require Internet service providers to maintain "a reasonable intercept capability, by means of a notice." This notice must comply with a "reasonable requirements" document, said Walsh. "Before publishing this document, there must be a consultation process involving all those the document is likely to affect. And the draft must be approved by both houses of Parliament," she said.

An Interception Commissioner, an independent judge, would oversee the use of this power for the first time. "An audit team will visit the law enforcement and intelligence agencies which acquire communications data, and examine the necessity and proportionality grounds behind the notice," according to the Home Office.

Walsh insisted the public would be consulted "before a procedure for handing over encryption keys is implemented." But, she added, "The government currently has no plans whatsoever to require anyone to install any equipment for the provision of communications data."

Nor would the law impose unreasonable financial or regulatory burdens on business, she said. "It will enable effective detection and investigation of crimes utilising the new technologies, including those committed against business itself," she said.

The order that defines the interception capability that Internet service providers should maintain "has been subject to consultation with industry and other interest parties and is currently with the European Commission," she said.

She said the Home Office intends to ensure that the law is in accordance with the due process clauses of the 1998 Human Rights Act, the U.K. law that implements the European Convention on Human Rights.

The Home Office is setting up a technical advisory board to look at the issues.

> "We are in the process of advertising for a chairperson and six members representing the interests of the communication service providers," said Walsh. "It was always our plan that these would be introduced in a slower time."

The British Chambers of Commerce (BCC) commissioned a panel of legal experts last year who concluded that there was "a clear need for a rigorous framework for the regulation of law enforcement access to communications media, including the Internet."

It added, however, that the provisions of the law, as originally proposed, could "justifiably be described as mass surveillance of Internet activities without judicial warrant or adequate oversight. It substantially increases the power of public authorities without correspondingly increasing the scope for oversight and accountability."

BCC spokeswoman Sally Low said that placing such regulation within the framework of the European Convention on Human Rights "is a welcome and necessary objective. Business requires confidence that efficient and effective policing of criminal activities is regulated by clear and well reasoned legislation."

She added that BCC was "broadly happy with the amendments to the law. We're adopting a wait-and-see approach and keeping an eye on it" during the consultation period, she said.

For more information: Information on RIPA can be at *www.homeoffice.gov.uk/ripa/ripact.htm* on the Home Office website.

UNITED STATES

Unintentional E-Mail Disclosure Leads to Online Privacy Violation

Federal Trade Commission Bureau of Consumer Protection Director J. Howard Beales III announced on January 18, 2002 an FTC settlement with Eli Lilly and Company (Lilly) for alleged violations of its online privacy policy (In re Eli Lilly and Co., FTC, No. 0123214, 1/18/02).

Speaking at a press conference, Beales said the charges stem from the company's unauthorised disclosure of sensitive personal information collected from consumers through its Prozac.com website. A Lilly employee sent an e-mail message announcing the termination of an e-mail reminder service and unintentionally disclosed the e-mail addresses of all 669 subscribers to each individual subscriber by including all of the recipients' e-mail addresses in the "To:" line of the message.

Beales emphasised:

> "Even the unintentional release of sensitive medical information is a serious breach of consumers' trust. Companies that obtain sensitive information in exchange for a promise to keep it confidential must take appropriate steps to ensure the security of that information."

Although the settlement does not impose any monetary fines or penalties against Lilly, the company will be required to take appropriate security measures to protect consumers' privacy. Beales noted that post-settlement violations would be subjected to penalties.

Lilly is a pharmaceutical company based in Indiana. It manufactures, markets, and sells various drugs, including the anti-depressant medication Prozac. The company operates the Prozac.com website, which the company promotes as "Your Guide to Evaluating and Recovering from Depression".

Challenged Conduct

The FTC alleged that despite its claims to the contrary, Lilly failed to take appropriate steps to protect the confidentiality and security of the personal information collected from consumers through its websites.

Several of Lilly's websites, including *www.prozac.com* and *www.lilly.com*, collect personal information from visitors. Between March 15, 2000, and June 22, 2001, Lilly offered the "Medi-messenger" e-mail reminder service. The service enabled consumers to design and receive personal E-mail messages reminding them to take or refill their medication. Once a consumer registered for Medi-messenger, the reminder messages were automatically e-mailed from Lilly to the subscriber at the e-mail address s/he had provided, and according to the subscriber's requested schedule, the FTC reported. The reminders were individualised e-mails and did not identify any other subscribers to the service.

A Lilly employee created a new computer program to access Medi-messenger subscribers' e-mail addresses. An e-mail message announcing the termination of the Medi-messenger service was sent on June 27, 2001. Unlike the previous

Medi-messenger communications, the June 27th e-mail message included all of the recipients' e-mail addresses in the "To:" line of the message. As a result, the employee disclosed to each individual subscriber the e-mail addresses of all 669 Medi-messenger subscribers.

Privacy Promises

The FTC's complaint included Lilly's privacy policies which claimed that the company employs measures and takes steps appropriate under the circumstances to maintain and protect the privacy and confidentiality of personal information obtained from or about consumers through its Prozac.com and Lilly.com websites.

The policies included statements such as, "Eli Lilly and Company respects the privacy of visitors to its websites, and we feel it is important to maintain our guests' privacy as they take advantage of this resource."

The FTC's complaint further alleged that Lilly's claim of privacy and confidentiality was deceptive because Lilly failed to maintain or implement internal measures appropriate under the circumstances to protect sensitive consumer information. This failure led to the company's unintentional June 27 disclosure of Medi-messenger subscribers' personal information (i.e., e-mail addresses). Specifically, the complaint stated that Lilly failed to:

- provide appropriate training for its employees regarding consumer privacy and information security;
- provide appropriate oversight and assistance for the employee who sent out the e-mail, who had no prior experience in creating, testing, or implementing the computer program used; and
- implement appropriate checks and controls on the process, such as reviewing the computer program with experienced personnel and pre-testing the program internally before sending out the e-mail.

The FTC indicated that Lilly's failure to implement appropriate measures also violated a number of the company's own written security procedures.

Proposed Settlement

The proposed settlement contains provisions designed to prevent Lilly from engaging in similar acts and practices in the future. The proposed settlement would bar Lilly from making misrepresentations about the extent to which the company maintains and protects the privacy or confidentiality of any personal information collected from or about consumers. Lilly would also be required to establish and maintain a four-stage information security program designed to establish and maintain reasonable and appropriate administrative, technical, and physical safeguards to protect consumers' personal information against any reasonably anticipated threats or hazards to its security, confidentiality, or integrity, and to protect such information against unauthorised access, use, or disclosure, the FTC reported.

In particular, Lilly would be required to:

- designate appropriate personnel to coordinate and oversee the program;
- identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of personal information, including any such risks posed by lack of training, and to address these risks in each relevant area of its oper-

ations, whether performed by employees or agents, including: management and training of personnel; information systems for the processing, storage, transmission, or disposal of personal information; and prevention and response to attacks, intrusions, unauthorised access, or other information systems failures;

- conduct an annual written review by qualified persons, within ninety (90) days after the date of service of the order and yearly thereafter, which shall monitor and document compliance with the program, evaluate the program's effectiveness, and recommend changes to it; and
- adjust the program in light of any findings and recommendations resulting from reviews or ongoing monitoring, and in light of any material changes to Lilly's operations that affect the program.

Lilly's security breach was the subject of a July 2001 petition from the American Civil Liberties Union requesting that the FTC investigate and take appropriate action to remedy the breach.

FTC Commissioner Orson Swindle remarked:

"Lilly should be respected for its long-standing efforts in development of its privacy practices, its acceptance of responsibility for the internal failures that resulted in the alleged violation of its privacy policy, and its willingness to take appropriate steps to correct those mistakes. I appreciate the company's leadership in cooperating with us to improve its security measures, and I believe the firm will fully carry out its commitments under the proposed order. Lilly's responsiveness and its efforts to improve corporate privacy practices can be a model for others to follow."

There will be an announcement about the proposed consent agreement in the Federal Register shortly. The agreement will subsequently be subject to public comment for 30 days. Comments should be addressed to: Secretary, FTC, 6th St. and Pennsylvania Ave., N.W., Washington, DC 20580.

The commission vote to accept the proposed settlement was 5-0.

The complaint and proposed consent order are available at *www.ftc.gov*—the FTC's website—and from the Consumer Response Center, Room 130, 600 Pennsylvania Ave., N.W., Washington, DC 20580; (202) 382-4357.

UNITED STATES

Privacy Outlook for 2002

Privacy appears to be back on the agenda for the second session. Industry is somewhat divided on the issue, a few companies favour limited legislation, while others worry that moving any measure could open the door for more sweeping action. Nonetheless, Representatives Cliff Stearns (R-Fla.) and W.J. "Billy" Tauzin (R-La.) say they will offer legislation, but it seems unlikely to satisfy the concerns of privacy advocates. They may instead prefer a measure from Senate Commerce Committee Chairman Ernest Hollings (D-S.C.).

Congress has been examining the issue of imposing broad new online privacy standards for the past few years and while it may be just as content to continue to debate the issue, some say legislation expected to be introduced in the House may find some life in the second session.

So far, Congress has dealt with privacy on a sector specific or issue specific basis through passage of such laws as 1998's Children's Online Privacy Protection Act, which restricts companies from collecting personal information about children without their parents' permission, and privacy provisions that were included in the 1999 Gramm-Leach-Bliley law.

Still, privacy advocates, lawmakers, and even some companies continue to argue that Congress needs to pass broader privacy legislation that would address the increasing use of the Internet to collect personal information about consumers. Numerous bills have been introduced in the 107th Congress to address the issue. But like many issues not directly related to responding to the September 11, 2001 terrorist attacks, privacy got swept aside in Autumn 2001.

Stearns, Tauzin Leading Effort

Still, two key lawmakers in October indicated their intention to address the issue. Representative Cliff Stearns (R-Fla.,), and Energy and Commerce Committee Chairman W.J. "Billy" Tauzin (R-La.) intend to introduce a bill this session that most expect will be more industry friendly than legislation that may be offered in the Senate by Commerce Committee Chairman Ernest Hollings (D-S.C.).

"I plan on developing privacy legislation in the coming weeks to serve as a platform for further discussion," Stearns, who chairs the Energy and Commerce Committee's commerce, trade and consumer protection panel, said in a statement issued in early January. He said he hopes to see a bill reported out by March.

Stearns said his bill will track an outline he released in October. The outline called for companies to notify consumers about what information is being collected and how it is being used. It also would provide consumers with an opportunity to opt out of having such information collected and used. In addition, it would preempt state privacy laws.

Tauzin recently pointed out the need to move quickly on a preemption clause, noting the potential for California to enact new privacy legislation. In a December speech at the Business Software Alliance's Global Tech Summit, Tauzin also indicated that their legislation would offer a baseline of privacy standards that would be tougher on the government than on industry.

Preemption a Carrot for Industry

Preemption of state laws is a key carrot for industry support of any privacy legislation. Industry officials often express concern about the potential burden of having to comply with several different state privacy standards.

"If we are going to have legislation in the area of data privacy ... there ought to be at the very least a national standard," said Harriet Pearson, IBM's chief privacy officer, who declined to comment on the proposed Stearns legislation.

However, some companies have come out in favour of limited privacy protections such as Hewlett-Packard and Intel. Scott Cooper, Hewlett-Packard's manager for technology policy, said the provisions outlined by Stearns offer a "good starting point". His company backed a notice and opt-out bill introduced in the 106th Congress by Senators John McCain (R-Ariz.) and John Kerry (D-Mass.).

Division in Business Community

There is still disagreement among industry officials about whether to support any legislation. Groups like the Information Technology Association of America (ITAA), which represents a broad range of information technology companies, do not favour legislation. ITAA President Harris Miller said he believes the concerns about state action are overblown.

"All this fear about balkanisation (at the state level) is a red herring," Miller said.

Many online companies that collect information are concerned that even a limited bill could become a magnet for broader protections opposed by the industry. For example, Amazon.com told the Senate Commerce Committee last summer that it could support legislation that required companies to provide notice and choice about information being collected, preempted state laws and applied to both online and offline activities. But the company would oppose a measure if it allowed individuals to sue companies for privacy violations.

Privacy advocates worry that a bad federal law that preempts state laws may be worse than no privacy legislation. The Stearns-Tauzin proposal appears to offer more to industry than consumers and would override the ability of states to pass more stringent protections, said Chris Hoofnagle, legislative counsel for the Electronic Privacy Information Center (EPIC), which favours privacy legislation and promotes free-speech rights.

"It's more than not doing something, it's doing something to stop states ... [from engaging] in their traditional role of protecting consumers," he said.

Hollings Refining Opt-In Approach

On the Senate side, aides to Hollings say he is still interested in pursuing a privacy bill that may require companies to allow consumers to "opt-in" before their personal information can be collected and used. "He wants an opt-in for personal identifiable information," said Hollings spokesman Andy Davis.

But Hollings is not expected to introduce the same legislation he offered in the 106th Congress, aides say. His old bill required firms to notify consumers about what information they seek to collect and get a consumer's permission before they collect and use it. Instead, Hollings has been negotiating to develop a new bill with broader appeal. His aides have been working with the staff for committee members that include Kerry and Senators Barbara Boxer (D-Calif.), Ron Wyden (D-Ore.), and Conrad Burns (R-Mont.).

One option under discussion would require an opt-in approach only for sensitive data such as financial information. Another controversial provision that Hollings included in his last bill would have provided consumers with a right to sue for privacy violations. Industry would likely oppose such provision and a strong opt-in component, observers state.

Prospects of Action in Doubt

Many of those following the debate say it is too early to say whether any privacy legislation has much hope for passage this session. Miller of ITAA said he believes the Stearns-Tauzin measure "may have some legs".

And another industry lobbyist predicts that if a bill reaches the House floor, lawmakers will have a tough time voting against a privacy bill in an election year.

House Majority Leader Dick Armey (R-Texas) has been interested in ensuring that enhanced security measures do not come at the expense of personal privacy, but he has not taken a position on Stearns potential legislation, an aide said.

But others are more sceptical, particularly if legislation does not move early in the session. Privacy legislation may find some life in the second session, but "whether it's going to translate into passed legislation is a different issue," said Ronald Plesser, a partner, who focuses on privacy issues, in the Washington office of the Piper, Marbury, Rudnick and Wolfe law firm.

He added that he is not sure if there is enough pressure yet to move privacy legislation. The Bush administration has not articulated a privacy policy, and has so far declined to name a new person to fill the job of White House privacy adviser that was created by former President Clinton. And Federal Trade Commission (FTC) Chairman Timothy Muris has said his agency plans to focus for now on enforcement, not new legislation.

Social Security Numbers

Meanwhile, several other privacy bills addressing various issues also have been introduced including measures to restrict the use of Social Security numbers. These include H.R. 91 sponsored by Representative Rodney Frelinghuysen (R-N.J.) and H.R. 1478 by

Rep. Jerry Kleczka (D-Wis.). But it remains to be seen whether they will see any action this year.

Stearns included language in his legislative outline that would place new restrictions on the use of Social Security numbers such as requiring the number holder's permission before selling or publicly displaying it except under certain conditions.

In the Senate, Senator Dianne Feinstein (D-Californian) has introduced a handful of privacy related bills, including a broad privacy bill (section 1055) and a narrower one (section 848), both of which would place new restrictions on the use and sale of Social Security numbers. Both of her bills have been referred to the Judiciary Committee. The Technology, Terrorism and Government Information Subcommittee, which Feinstein chairs, may hold a hearing early in the session, according to a committee aide.

UNITED STATES

"Don't Call" Registry Under Amendment to Telemarketing Rule

The Federal Trade Commission (FTC) on January 22, 2002 proposed to create a centralised national "Do Not Call" registry so that consumers may eliminate most telemarketing calls with one toll-free phone call. This is one facet of the proposed amendments to the Telemarketing Sales Rule (TSR).

During the January 22 press conference announcing the proposals to amend the regulation, J. Howard Beales III, Director of the FTC's Bureau of Consumer Protection, indicated that, under one proposal, telemarketers would be barred from calling all consumers who place their names on this national registry.

Other proposed changes to the TSR include prohibiting telemarketers from trafficking in consumers' credit card and other account numbers; barring telemarketers from blocking or otherwise subverting caller ID systems; and implementing the Patriot Act, which requires the FTC to regulate calls made by for-profit telemarketers to solicit charitable contributions.

The FTC is seeking comments from consumers and telemarketers for the next 60 days. Beales indicated that "the rulemaking process can be a long one, and today's announcement is the first step in that process. It will be a while before these proposals can be a reality."

The current TSR provisions, such as restrictions on the time telemarketing calls may be placed, remain in effect until the rule is amended, Beales emphasised. He declared:

> "We know that consumers are concerned about their privacy, that includes unwanted intrusions—those annoying occurrences that disrupt a person's daily activities—unwanted phone calls at the dinner hour for example, it also includes the misuse of their personal information which can have serious economic consequences. Those are the reasons for the 'Do Not Call' proposals and the restrictions on pre-acquired account information. The proposed changes address these privacy concerns."

Privacy is the major concern of both the FTC and consumers, he stressed. Beales expressed confidence that these proposals will help protect privacy in very real and meaningful ways.

The proposed amendments to the TSR are available at *www.ftc.gov*—the FTC's website—and from the Consumer Response Center, Room 130, 600 Pennsylvania Ave., N.W., Washington, DC 20580; (202) 382-4357.

UNITED STATES

Privacy Group Sues FBI To Release Purchase Records

The Electronic Privacy Information Center (EPIC) is suing the Federal Bureau of Investigation (FBI) and five other federal agencies to force them to release records relating to their purchase from private companies of personal information about individuals.

EPIC, an advocacy group that promotes privacy protections and free speech rights, filed its lawsuit on January 14, 2002 in the U.S. District Court for the District of Columbia against the FBI, the Drug Enforcement Administration, the U.S. Marshals Service, the Internal Revenue Service, the Immigration and Naturalisation Service, and the Bureau of Alcohol, Tobacco and Firearms.

EPIC is claiming that the agencies have violated the law by failing to respond to the group's Freedom of Information Act requests for records relating to "transactions, communications, and contracts" about the sale of personal information to the agencies by two private companies, ChoicePoint and Experian.

Chris Hoofnagle, EPIC's legislative counsel, said his group wants to know what type of information is being sold to the government agencies and whether there is a danger for misuse of the data. Current law limits the ability of law enforcement agencies to create dossiers on U.S. citizens, Hoofnagle said. But he added that his group is concerned that purchasing personal information from private companies may be a way of bypassing the law.

EPIC said it has documents that show the IRS was sold state motor vehicle records, marriage and divorce data, international asset location data, and credit header data, which includes a person's name, address, phone number, date of birth and Social Security number.

"There is problems on both sides, with the purchase of personal information (by the agencies), which is happening without much public awareness and oversight, and with the private sector building profiles on consumers," Hoofnagle said.

UNITED STATES

Health Insurers Analyse State Privacy Laws

The Health Insurance Association of America, Shaw Pittman LLP, and the Blue Cross Blue Shield Association have partnered to develop a comprehensive analysis of the state medical privacy laws, the groups announced in a January 17, 2002 press statement.

This 50-state analysis will help health plans and other health care organisations toward compliance with the federal privacy regulation, which took effect in spring 2001.

The medical privacy regulation issued on December 28, 2000 (65 Fed. Reg. 82461) and mandated by the 1996 Health Insurance Portability and Accountability Act (HIPAA) serves as a federal floor of protection and allows states to pass stronger laws to regulate the disclosure of patient medical information. Compliance with the HIPAA privacy regulations is required by April 14, 2003.

To comply with the HIPAA privacy regulation as well as state privacy requirements, health care organisations will need to determine whether state or federal laws or regulations will apply in any given situation, health care experts have said. Officials from the Department of Health and Human Services, the agency that promulgated the rule, have said that HHS does not have the authority or resources to prepare an analysis of state laws and how they will interact with the federal privacy regulation.

In the state-by-state analysis, the health care insurers and the law firm will seek to compare the requirements of the HIPAA privacy regulations with state health-related privacy statutes and regulations, and show which requirements health plans should follow, according to the January 17 statement.

Other groups, including a task force at the American Bar Association (ABA), have attempted to analyse state laws and compare them with the federal privacy rule and have concluded the task is very difficult because state laws will continue to change.

Additionally, the ABA task force found that health care groups that must comply with the rule will have to pay attention to state laws on medical records, genetic testing, mental health, and substance abuse. Health care organisations also have to review state health and safety codes as well as pharmacy and licensure laws.

The HIAA/BCBSA/Shaw Pittman analysis should become the national standard for assessing when HIPAA preempts state laws, the groups said in their statement. They expect the analysis to be available in May 2002. It is planned to be a subscription service available in printed form and as a fully searchable electronic database, both online and on a CD-ROM. The groups plan to update the analysis quarterly starting July 2002 for an additional fee.

For more information about the state privacy law analysis, call the Health Insurance Association of America at (202) 663-8800 or send an e-mail to hipaaready@hiaa.org.

UNITED STATES

U.S. Government Creating Computer Spy Viruses

According to published reports, the United States government is developing a new way to spy on Internet users, through the use of computer viruses.

The US Federal Bureau of Investigations has confirmed that it is working on Magic Lantern technology to help spy on computer users. While precise details have been hard to come by, the system allegedly includes a special virus that allows the attacker to log each and every keystroke that is typed into a target machine. The technique could be used to steal passwords and read private documents stored on a targeted person's computer. The use of viruses would make it easier for law enforcement agents to install keylogging devices on individuals' machines without having to physically break into people's homes or offices, which the U.S. government has done in the past (as mentioned in the recent case of *Nicodemus Scarfo*).

Not surprisingly, these revelations have been met with condemnation from many experts, who worry that the system may not only allow unnecessary government intrusions into cyberspace, but may also undermine general computer security. In addition, questions have been raised as to whether the anti-virus software manufacturers would comply with the U.S. government's requests for assistance by leaving users unprotected against Magic Lantern attacks. Several of these companies have said that they would need a court order before going along with any such FBI demands.

In the latest development, U.S. Representative Ron Paul is pressuring the FBI to provide more details about Magic Lantern. Paul noted in a letter to the Bureau that his "legislative director attempted to obtain information on this project from the FBI and was told such information was classified." He warned that if "media reports are accurate, the Magic Lantern project could greatly impact the privacy and civil liberties of all Americans who communicate via e-mail," and that he was "disturbed" by the FBI's stonewalling. The congressman insisted that the agency release information about the project or at least provide him "with written justification for the FBI's refusal to share information on this crucial issue."

See Robert MacMillan, "Lawmaker Wants Magic Lantern Information From FBI", Newsbytes, January 14, 2002 at *www.newsbytes.com/news/02/173637.html*.

UNITED STATES

More Security Problems Dog Microsoft

Over the past few months, security experts have discovered flaws in a variety of Microsoft products.

Some of these breaches were quite serious. One such defect in Windows XP could have permitted scam artists to make use of the operating systems' Universal Plug and Play feature to take over victims' computers. Another major flaw, this time in Microsoft's Internet Explorer 6, would have allowed an attacker to access private files, steal cookies and even redirect the targeted user along the World Wide Web.

Additionally, privacy guru Richard M. Smith demonstrated how a hole within Windows Media Player can be used to track users of IE6, even if they have Microsoft's vaunted P3P (Platform for Privacy Preferences) technology on a high setting. The software giant has released patches for most but not all of these vulnerabilities, and Smith has criticised Microsoft's approach to fixing the Media Player hole in particular as inadequate: "There are many people who have never run Windows Media Player yet they are still vulnerable to the problem."

These discoveries have made many observers wonder whether the company is doing enough to protect the privacy of its customers. Indeed, several organisations, including the Electronic Privacy Information Center, Computer Professionals for Social Responsibility, the Electronic Frontier Foundation and NetAction, had made similar points in a series of complaints to the United States Federal Trade Commission. Meanwhile, a few insurance companies have taken the unusual step of charging policyholders who use a large number of Microsoft products higher premiums. See *www.gilc.org.*

UNITED STATES

Screening Of Airline Passengers Raises Privacy Concerns

Federal aviation authorities and technology companies are to begin testing a vast air security screening system designed to instantly pull together every passenger's travel history and living arrangements, plus a wealth of other personal and demographic information, according the an article in The Washington Post (February 1, 2002).

The government's plan is reportedly to establish a computer network linking every reservation system in the United States to private and government databases. The network would use data-mining and predictive software to profile passenger activity and intuit obscure clues about potential threats, even before the scheduled day of flight.

Although such a system would rely on existing software and technology, it could be some years before it is ready, as enormous amounts of data need to be integrated and a structure established for monitoring passenger profiles.

The screening plans are said to reflect a growing faith among aviation and government leaders that information technology can solve some of the nation's most vexing security problems by rooting out and snaring people who intend to commit terrorist acts.

Fears for Privacy

However, a range of policy and technical questions still need to be answered before the system can become a reality. The Transportation Security Administration (TSA), for example, must decide on a set of standards so technology companies and airlines can begin building a system. They must work out how to pay for the system and its operation. Officials at the TSA are reluctant to comment as they do not want to disclose details that might undermine aviation security. Government officials and companies have also faced questions about privacy. But developers may be restricted as to how much information they can use. Industry officials have already discussed with lawmakers the possible need to roll back some privacy protections in the Fair Credit Reporting Act and Driver's Privacy Protection Act to enable them to use more of the credit and driver's licence data.

Civil liberties activists are concerned that the system could be the start of a surveillance infrastructure that will erode existing privacy protections. Some critics also fear that law enforcement authorities will be tempted to use it for broader aims. Richard M. Smith, an independent computer security and privacy specialist said:

> "The computer technology is so cheap and getting so much cheaper, you just have to be careful: Turn up the volume a little bit, and we just use the air transportation system to catch everybody."

Prototypes Being Developed

Two leading prototypes are reportedly being developed. One group is led by HNC Software, a risk-detection specialist that works for credit card issuers, telephone companies, insurers and others. HNC is working with several companies, including PROS Revenue Management, which has access to seating records of virtually every U.S. passenger, and Acxiom Corp., one of the world's largest data-marketing companies, which collects such information as land records, car ownership, projected income, magazine subscriptions and telephone numbers. A second group is being led by Accenture. It has worked for months on a prototype with a variety of companies, including Delta. Equifax, Sabre Inc. (which is responsible for about half of U.S. airline reservations), IBM and other companies have also been working on profiling efforts.

Both systems are designed to use travel information and other data to create models of "normal" activity. Then they will look for variations in individual behaviour that might suggest risk. Both may eventually make use of some sort of biometric system that uses iris scans, fingerprints or other immutable characteristics. See *www.washingtonpost.com*.

UNITED STATES

Administration Stays on Sidelines of Privacy Debate

First published in Pike & Fischer's Internet Law & Regulation (http://internetlaw.pf.com)

The Bush administration has not developed a set of privacy policy principles and does not plan to wade into the debate over whether Congress should enact new privacy rules until major legislation is introduced, a Commerce Department official said on January 31, 2002.

Despite warning industry leaders to carefully consider the implications of privacy legislation, Chris Israel, the Commerce Department's deputy assistant secretary for technology policy, said the administration had not formulated a policy yet and would wait to see what Congress does on the issue. Israel was one of a handful of administration officials who spoke at a three-day conference in Washington, D.C. on privacy sponsored by the International Association of Privacy Officers.

Israel said the administration is focused on a "balanced approach to privacy" that is open to innovation, but he did not elaborate on what this would include.

When asked whether the administration would favour legislation that would prevent state privacy laws—a key component in attracting business support for privacy legislation—Israel said the administration "understands the ramifications that a proliferation of state laws could have" on companies but has not taken a position on the issue yet, he said.

The Federal Trade Commission (FTC), the lead agency charged with enforcing consumer rights, has so far indicated it will not push for privacy legislation. Unlike his predecessor from the Clinton administration, FTC Chairman Timothy Muris has indicated the agency will focus instead on enforcement of current laws. Under the leadership of former Chairman Robert Pitofsky, the FTC advocated passage of privacy legislation.

FTC Commissioner Mozelle Thompson, however, said while enforcement is important, he disagrees with those who say legislation is not needed right now.

> "I still believe there is a benefit [in] having some legislation that provides a privacy baseline," he said.

He also took issue with the new chairman's decision to shift the agency's focus away from the collection of personal information and toward a heavier focus on misuse of such information, He said such a move shifts the risk back on to the consumer.

Online-Offline Controversy

Howard Beales, director of the FTC's consumer protection bureau, discussed a recent controversy he sparked when he said that privacy policies posted by companies online apply to their offline practices as well.

He reiterated his claim that he was not unveiling a new policy but added that some of the confusion might have stemmed from the agency's past heavy focus on online privacy protections.

> "This straightforward adaptation of deception law is only news because of the artificial limitation of focusing on online privacy rather than privacy in general," Beales said.

He warned companies that if they want to make a distinction between their online and offline privacy practices, they "need to make sure the limitation is as clear as the claim."

He added that unless companies take such a step, "reasonable consumers are going to assume the claim applies to all information practices, not just some. We will make the same assumption."

Financial Privacy, Antiterrorism

Other administration officials addressed narrower aspects of the privacy debate. Amy friend, assistant chief counsel from the Office of the Comptroller of the Currency, discussed the "potency" of financial privacy and some of the circumstances that led to the inclusion of new privacy rules in the Financial Services Modernisation Act passed in 1999. The law requires companies to notify consumers about what personal information the companies share with unaffiliated third parties and to provide consumers with a chance to opt out of such arrangements.

The notices sent out by financial services companies, however, have come under fire for being difficult to read and comprehend. Friend said her agency is discussing developing a two-tier notification system that would involve sending out a shorter, easier-to-read notice that clearly explains the most important points for consumers along with a much longer explanation of consumer rights under the law. "We want to encourage that approach," she said.

Daniel Collins, the Justice Department's chief privacy officer, defended provisions dealing with electronic privacy that were included in antiterrorism legislation passed in Autumn 2001. He reiterated the administration's claims that the provisions amending wiretap laws do not expand law enforcement powers, as some critics claim, but instead update current laws to make them technology-neutral.

"Critics [of the law] are wide off the mark" in describing the law's potential threats to privacy, Collins said.

CASE REPORTS

COLOMBIA

■ PROVISION IMPOSING OBLIGATIONS UPON WEBSITES DECLARED CONSTITUTIONAL IN PART

Judgment C-1147 of 2001

Constitutional Court, October 31, 2001

Report by Daniel Peña, director of the IT Group of Cavelier Abogados (www.cavelier.com), Bogotá; e-mail: danielpena@cavelier.com

The Colombian Constitutional Court declared that the provision regulating the mercantile registry of Internet websites in chambers of commerce should be adjusted to the National Constitution, and authorised tax authorities to request information on electronic transactions.

However, the Court required the Colombian authorities to observe certain conditions at the time of enforcing such provision: that they shall respect the principle of ultimate purpose, the principle of relevance, the right to privacy and the *habeas data* of the agents involved.

The case originated from a complaint filed by a citizen against a provision which had existed for over one year in Colombia, which ordered that every website and Internet page of Colombian origin operating on the Internet should submit to the National Directorate of Customs and Taxes (DIAN) all the information it may request. The citizen considered that the provision infringed the Constitution, since it gave excessive power to the tax authority and, additionally, it imposed an obligation which appertained to commercial law (the mercantile registry) without there being, in his opinion, a relationship between the two subject matters.

The Court, notwithstanding, rejected the complaint regarding the provision being incompatible with the Constitution, to the extent that it is limited to imposing, upon one single person, whether natural or legal, engaged in rendering personal, commercial or financial services, in whole or in part, through the web, the duty to comply with certain administrative, commercial and taxation duties which the rest of the citizens must meet when performing those activities.

However, the Court nevertheless imposed conditions on the powers of the tax administration, which it required to respect the following rights:

(a) the right to privacy of those who perform electronic transactions, since in matters relating to tax inspection, the tax administration cannot demand such information which due to its connotations and characteristics appertains exclusively to the sphere of private interest of the individual;

(b) the principle of relevance, which in each concrete case it is assumed that solely the information relating to the functions legally attributed to the requiring entity may be required and disclosed. For example, if the DIAN is investigating an establishment engaged in the sale of books and magazines through the Internet in general terms, requesting information as to the names of purchasers of specific types of products would infringe the principle of relevance;

(c) the principle of ultimate purpose, in such a manner that the information requested and disclosed is:

- strictly necessary for meeting the purposes of the administration in the particular case, and
- exclusively used for the purposes authorised by law, which in the present context are related to inspection, collection, determination, discussion and administration of taxation matters within the specific terms established by legal provisions for each particular tax.

In light of the foregoing, the Court declared invalid that portion of the provision that obliges private individuals to disclose information about all and every one of their transactions in an unlimited manner, since it permits an officer of the administration to be in charge of choosing the content and extent of an obligation which may only be established by the lawmaker.

This judgment is important to the extent that it provides greater clarity about the manner in which Internet websites shall be registered with the authorities, and it establishes the required limitations on tax authorities concerning the information they may obtain about on-line transactions in Colombia.

HUMAN RIGHTS COURT

■ PHONE TAPS IN THE DETECTION OF CRIME

PG and JH v. United Kingdom

European Court of Human Rights. September 25, 2001

The European Court of Human Rights has ruled on the legality of surveillance techniques used by the United Kingdom Government in the course of an investigation into a criminal conspiracy.

The police had received information that an armed robbery was about to take place. In order to obtain further details, an application was made for a covert listening device in B's flat where the applicants were observed

going in and out. Guidelines issued by the Home Office in 1984 required written authorisation. Instead oral confirmation was given by the Chief Constable to install the device and retrospective written authorisation was given only four days later. British Telecom also supplied an itemised billing to the police in relation to B's telephone calls at the critical period.

The robbery never took place as the listening device was discovered. However, B as well as the applicants were arrested and all the tools necessary to commit the crime were discovered in the flat and in the boot of their car. B pleaded guilty.

In order to obtain speech samples, which the applicants had refused when arrested—so as to compare with the tapes from the device in B's flat—the police applied for and received written authorisation to install covert listening devices in the applicants' cells, as well attaching them to the officers present when they were charged. Thus the samples were recorded without the applicants' permission or prior knowledge. They were convicted and sentenced to 15 years' imprisonment and refused leave to appeal to the Court of Appeal.

Appeal to Human Rights Court

The court said that, of the several issues which arose, the applicants, inter alia, invoked Article 8 of the Convention, which provides insofar as relevant as follows:

> "1.Everyone has the right to respect for his private ... life, ... and his correspondence.
>
> 2.There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of ... public safety ..., for the prevention of disorder or crime, ... or for the protection of the rights and freedoms of others."

Under the Home Office Guidelines 1984 authority can be given for the use of listening devices, inter alia, where an investigation concerned a serious crime and where there was good reason to think that the use of the equipment would assist in leading to arrest and conviction. However, the intrusion into the privacy of those affected had to be commensurate with the seriousness of the offence.

The Police 1997 Act, which entered in to force in February 1999, provides for a statutory basis for the authorisation of police surveillance operations involving interference with property or wireless telegraphy. Since September 2000, those controls have been augmented by Part II of the Regulation of Investigatory Powers Act 2000 ("RIPA"). In particular, covert surveillance in a police cell is now governed by sections 6(3) and 48(1) of RIPA. RIPA also establishes a statutory Investigatory Powers Tribunal to deal with complaints about intrusive surveillance and the use of informants by the police.

Section 45 of the Telecommunications Act 1945 prohibits the disclosure by a person engaged in a telecommunications system of any information concerning the use made of the telecommunications services for any other person.

However, pursuant to section 28(3) of the Data Protection Act 1984:

> "Personal data are exempt from non-disclosure provisions in any case for the purpose of: the prevention or detection of crime, or the apprehension or prosecution of offenders."

Use of Covert Listening Device

The applicants had submitted that the use of a covert listening device at B's flat to monitor and record conversations was an interference with their rights under Article 8(1) which was not justified under the second paragraph of that provision. At the time of the events in their case there existed no statutory system to regulate the use of covert listening devices, although the Police Act 1997 now provided such a framework. The Home Office Guidelines which provided the relevant instructions to the police were neither legally binding nor directly publicly accessible.

In *Khan v United Kingdom (no. 35394/97, [Section 3], ECHR 2000-V,* the Court found that the Home Office Guidelines governing such devices did not satisfy the requirement of "in accordance with the law". In the judgment of the Court, it was not disputed that the surveillance carried out by the police at B's flat amounted to an interference with the right of the applicants to respect for their private life.

As regards conformity with the requirements of the second paragraph of Article 8(2)—that any such interference be "in accordance with the law" and "necessary in a democratic society" for one or more of the specified aims—there was no domestic law regulating the use of covert listening devices at the relevant time (see *Khan v United Kingdom*). Thus the interference in this case was not "in accordance with the law" as required by Article 8(2) of the Convention, and there had been a violation of Article 8.

Information on Use of Telephone

The applicants also submitted that the metering of the telephone in B's flat constituted an interference with their rights under Article 8. While the Government acknowledged that those who used the telephone had an expectation of privacy in respect of the numbers which they dialled, the obtaining of the information was necessary in all the circumstances of the present case.

The information obtained concerned the telephone numbers called from B's flat between two specific dates. It did not include any information about the contents of those calls, or who made or received them. The data obtained, and the use that could be made of it, were therefore strictly limited.

Disclosure to the police was permitted under the relevant statutory framework where necessary for the purposes of the detection and prevention of crime and the material was used at the applicants' trial on criminal charges to corroborate other evidence relevant to the

timing of telephone calls. Therefore the measure in question was "in accordance with the law" and that there had been no violation of Article 8.

Use of Listening Devices in Police Station

With regard to the secret recordings when the applicants were being charged in the police station and when they were held in their cells, they submitted that it was irrelevant what was said, which ranged from the giving of personal details to a conversation about football instigated by a police officer. They considered that it was the circumstances in which the words were spoken which was significant and that there was a breach of privacy if the speaker believed that he was only speaking to the person addressed and had no reason to believe the conversation was being broadcast or recorded. In the present case, the police knew that the applicants had refused to provide voice samples voluntarily and sought to trick to them into speaking in an underhand procedure which was wholly unregulated. It was also irrelevant that the recording was used for forensic purposes rather than to obtain information about the speaker, as it was the covert recording itself, not the use made of it, which amounted to the breach of privacy.

"Private life" was a broad term not susceptible to exhaustive definition. While it was generally the case that the recordings were made for the purpose of using the content of the conversations in some way, the Court was unpersuaded that recordings for use as voice samples could be regarded as falling outside the scope of the protection afforded by Article 8. Though it was true that when being charged the applicants answered formal questions in a place where police officers were listening to them, the recording and analysis of their voices on this occasion still ought to be regarded as concerning the processing of personal data about the applicants.

The recording of the applicants' voices when being charged and when in their police cell disclosed an interference with their right to respect for private life within the meaning of Article 8(1) of the Convention.

In considering whether the interference was "in accordance with the law," there were two main requirements: (a) that there be some basis in domestic law for the measure and (b) that the quality of the law was such as to provide safeguards against arbitrariness.

While it might be permissible to rely on the implied powers of police officers to note evidence and collect and store exhibits for steps taken in the course of an investigation, it was trite law that specific statutory or other express legal authority was required for more invasive measures, whether searching private property or taking personal body samples. If there was a lack of any express basis in law for the interception of telephone calls on public and private phone systems or for covert surveillance devices on private premises, the requirement of lawfulness was not met. There was no material difference where the recording device was operated, without the knowledge or consent of the individual concerned, on police premises. The underlying principle that domestic law should provide protection against arbitrariness and abuse in the use of covert surveillance techniques, applied equally in that situation.

The Court noted that Regulation of Investigatory Powers Act 2000 contains provisions concerning covert surveillance on police premises. However, at the relevant time, there existed no statutory system to regulate the use of covert listening devices by the police on their own premises.

UNITED KINGDOM

WHEN PUBLIC INTEREST OUTWEIGHS PROTECTION OF PRESS CONFIDENTIALITY

Interbrew SA v. Financial Times and Others

Chancery Division, January 4 2002

The U.K. High Court has ruled on the competing interests between the public interest and the need to protect the press from having to reveal its sources. The court had to conduct a balancing exercise in light of the inter-relationship of Article 10 of the European Convention on Human Rights—guaranteeing the right to freedom of expression—and section 10 of the Contempt of Court Act 1981which provides for protection from disclosure of sources unless a court is persuaded that disclosure is necessary in the interests of justice.

The interlocutory hearing resulted from events in a possible takeover bid by the claimant. A confidential and market sensitive document was produced for consideration by the claimant but, at some point, a person, whose identity remained unknown ("the source"), obtained a copy of it and prepared a "doctored" version. Most importantly that version fabricated an offer price and timetable for the bid. The source then distributed it to various publishers of news, including the five defendants, viz. Financial Times, Independent, Guardian, Times and Reuters, in order to create a false market in the shares. The items were variously printed and the impact on the market was significant.

The "doctored" documents were thus in the public domain but the claimant, in an endeavour to trace the source of the leak and the falsification of the information, required the defendants to deliver up the original copies received.

The Court's Conclusions

Mr. Justice Lightman said that the Court should always start with a presumption that it was contrary to the public interest to require disclosure of sources unless an overriding public interest required otherwise. However, the weight of competing interest to displace that presumption depended on the circumstances of the partic-

ular case. The onus was thus on the claimant to establish that it would use the documents to identify the source as the means of removing a continuing threat of damage to its business and that the achievement of this aim was so important that it overrode the public interest.

The principle established in the case of *Norwich Pharmacal v. Customs & Excise Commissioners [1974] AC 133 at 175* and restated by Lord Phillips in *Ashworth v. MGN [2001] 1 WLR 515 at paragraph 42*) provided that, where a person through no fault of his own got mixed up in the wrongful acts of others (for which purpose it was irrelevant whether the wrong was tortious or a breach of an equitable obligation) so as to facilitate their wrongdoing, though he might incur no personal liability, came under a duty to assist the person who had been wronged by giving him full information and disclosing the identity of the wrongdoer. Justice required that he should cooperate in righting the wrong if he unwillingly facilitated its perpetration.

There were two implicit limitations upon the application of the principle. First the obligation did not extend to mere witnesses or persons who merely happened to have possession of relevant evidence: the obligation extended only to those who are involved in or facilitated the wrongdoing: *Ricci v. Chow [1987] 1 WLR 1658*. Secondly there might be a rule of public policy which precluded application of the principle in the circumstances of a particular case.

Defendants Obliged to Cooperate

It was quite clear on the facts that the Defendants through no fault of their own got mixed up in the wrongful acts of the source so as to facilitate the source's wrongdoing. The source set out to feed the Defendants in the form of the doctored copies with confidential information (that the Claimant was considering a takeover bid and had prepared a report on the project) mixed with deliberately false information regarding bid price and timetable. The aim was to manipulate the press and through the press to make a false market in the shares. The Defendants were not mere witnesses. Their receipt of the doctored copies and their publication of articles based on it were essential parts of the source's scheme. The Defendants accordingly fell within the ambit of grant of *Norwich Pharmacal* relief.

The important principle that the public perception that the press would in any ordinary circumstances keep confidential its sources could not sustain any real damage where it is encroached upon in the exceptional circumstances of the present case.

No fair-minded observer could reasonably take the view that a person acting as the source had should be protected from identification by press privilege. Indeed it could be thought to bring that privilege into disrepute and be an affront to justice and common sense it was available to preclude enquiries which would prevent a repetition of fraud upon the public.

UNITED STATES

SUPREME COURT REFUSED TO REVIEW PRIVACY CLAIMS DECISION

Consolidated Freightways Inc. v. Cramer, U.S. (No. 01-432)

U.S. Supreme Court (9th Circuit), Certificate denied January 7, 2002

The U.S. Supreme Court on January 7, 2002 declined to review an appeals court decision that state law claims brought by approximately 274 union-represented employees who were secretly recorded in a workplace restroom are not preempted by the Labor-Management Relations Act.

The full U.S. Court of Appeals for the Ninth Circuit ruled that the employees can proceed with invasion of privacy and intentional infliction of emotional distress claims against Consolidated Freightways Inc. (255 F.3d 683 (9th Cir. 2001)). The court ruled 10-1 on the privacy claims and 9-2 on the emotional distress claims. The trucking company concealed video and audio recording devices behind two-way mirrors in the restrooms of its terminal in Mira Loma, California, in an effort to catch drivers using drugs. Employees discovered the equipment when a mirror fell off a wall. Reversing a lower court's dismissal of the employees' claims, the appeals court found that the claims "are not even arguably covered by the collective bargaining agreement" between Consolidated and International Brotherhood of Teamsters Local 63.

The appeals court clarified the analysis that should be used in determining whether state law claims are preempted by LMRA Section 301, which gives federal courts jurisdiction to decide suits alleging breach of a collective bargaining agreement. California criminal law makes it a misdemeanour to install or maintain a two-way mirror allowing observation of a restroom or to use electronic devices to eavesdrop on confidential communications.

The dissent maintained that the claims should be preempted because a contract provision allowing video surveillance in certain circumstances could be "reasonably interpreted to affect materially the resolution" of the state law claims.

An appeals court panel previously had ruled 2-1 that the claims were preempted by the LMRA (209 F.3d 1122 (9th Cir. 2000). The panel majority found that the employees' claims turned on their reasonable expectation of privacy, which may have been bargained away in the contract.

Signs Warned of 24-Hour Surveillance

In its petition for Supreme Court review, Consolidated noted that the contract allows a supervisor with probable suspicion to require an employee to undergo drug testing. Another provision states that the company

"may not use video cameras to discipline or discharge an employee for reasons other than theft of property or dishonesty" Six large signs posted in and around the Mira Loma terminal warned employees that they were subject to 24-hour surveillance recorded on videotape, the company said.

Citing Supreme Court precedent on section 301 preemption, Consolidated argued that resolution of the employees' claims "plainly requires an interpretation of the [collective bargaining agreement] in this case." To prevail on the invasion of privacy claims, the employees would have to show they had a reasonable expectation of privacy in the restrooms, which would be affected by whether and to what extent they consented to the video surveillance by agreeing to the contract, the company said.

The Ninth Circuit en banc ruling "conflicts with the decisions of every circuit that has considered whether § 301 preempts claims for invasion of workplace privacy," Consolidated argued. The Seventh Circuit held in *In re Amoco Petroleum Additives Co., 964 F.2d 706 (7th Cir. 1992)*, that employees' claims of invasion of privacy and infliction of emotional distress based on an employer's use of a hidden video camera were preempted even though the collective bargaining agreement did not say anything about surveillance, Consolidated said.

The company argued that the Ninth Circuit ruling "also conflicts with numerous decisions of other circuits" recognising that section 301 preempts claims involving a condition of employment such as workplace privacy that is an ordinary subject of bargaining, because the contract might deal with such matters by implication.

E. Barrett Prettyman of Hogan & Hartson in Washington, D.C., was the counsel of record for Consolidated.

Cannot Bargain for Illegal Conduct

Citing *Allis-Chalmers Corp. v. Lueck, 471 U.S. 202 (1985)*, the employees argued in their brief opposing Supreme Court review that "a collective bargaining agreement cannot allow conduct that is illegal under state law." Consolidated's actions "are an obvious violation of California law, and there is no reason to interpret the collective bargaining agreement to determine the legality of [the company's] actions," the employees said. They also argued that it is unnecessary to interpret the contract to determine whether they had an expectation of privacy because California law provides "users of a restroom with a reasonable expectation of privacy as a matter of law."

The Supreme Court repeatedly has held that bargaining contract waivers of state law rights must be clear and unmistakable, the employees said.

> "In the present case, even a cursory look at the collective bargaining agreement shows that it is silent on the subject of placement of cameras in violation of state laws, so there is no 'clear and unmistakable' waiver of privacy rights in this case," the employees asserted.

Disputing Consolidated's claim of a conflict among the circuits, the employees argued that the Ninth Circuit's ruling "is entirely consistent with the oft-repeated rule from other circuits that the LMRA does not preempt state lawsuits arising from activities prohibited by state law." The cases cited by Consolidated involve employer conduct that is legal under state law, the employees said.

Matthew L. Taylor of Myers, Taylor & Siegel in Claremont, California, was the counsel of record for the employees.

COMMENTARY

ITALY

Corrective Provisions on Data Protection

By Avv. Alessandro del Ninno, Studio Legale Tonucci, Via Principessa Clotilde n. 7 00196 Rome. E-Mail: adelninno@tonucci.it.

With the publication of the Legislative Decree No. 467/2001 in the Italian Official Journal No. 13 of January 16, 2002 important corrective and supplementary provisions with regard to the Italian Law on Privacy of December 31, 1996 No. 675 "*Protection of individuals and other subjects with regard to the processing of personal data*" have been introduced.

It should be pointed out that when the Law No. 675 was enacted in 1996, the Italian Parliament had adopted at the same time a specific delegated law enabling the Government to successively correct and supplement—every two years—the Italian Law on Privacy No. 675/1996 (Law of December 31, 1996 No. 676 "*Act enabling the Government in the field of the protection of individuals and other subjects with regard to the processing of personal data*", Link (in English) for the text at: *http://astra.garanteprivacy.it/garante/prewiew/0,1724,448,00.html?sezione=120&LANG=2 (or www.garanteprivacy.it/garante).*

Since 1996 the measures necessary to exercise the delegation by the Government have been deferred several times, the last act being the Law of March 24, 2001 No. 127 (Law of March 24, 2001 No. 127 "*Deferment of the terms to exercise the delegation pursuant to Law of September 31, 1996 No. 676 with regard to the processing of personal data*" published in the Italian official Journal No. 91 of April 19, 2001. Link (in Italian) at: *www.privacy.it/legge2001127.html*).

According to this Law, the Parliament has renewed the delegation and—beyond others—has enabled the Italian Government to issue by December 31, 2002 a "Consolidation Act" which will codify and gather in a unique legislative text all the Italian provisions on personal data protection.

On the basis of the Law 127/2001, the Italian Government has enacted the Legislative Decree of December 28, 2001 No. 467 "*Corrective and supplementary provisions related to the Data Protection laws according to article 1 of Law of March 24, 2001 No. 127*" (Link (in Italian) for the text: *www.gazzettaufficiale.it*.

The new provisions will come into force on February 1, 2002. As a general consideration with regard to the modifications introduced, it can be said that a great simplification of the measures originally required by the Law 675/1996 (now amended by the Legislative Decree 467/2001) has been set up.

Scope of the Law

It is now provided that the Law 675/96 shall apply also to the processing of personal data carried out by subjects settled in territories outside the EU if these subjects process personal data by means of devices (electronic or non electronic) localised in Italy. In this case, these subjects need to appoint a representative settled in Italy. This provision shall not apply if the devices settled in Italy are only used for the aim of transit of processed personal data within the territory of the EU. This new principle has been added to article 2 of the Law 675/1996 which previously only provided this general rule: "This Act - (i.e.: Law 675/1996) - shall apply to the processing of personal data carried out by any person whomsoever on the State's territory".

Notification of Processing of Personal Data

A very important corrective provision has been introduced with regard the notification (in advance) of the processing of personal data to the Italian Authority for the Protection of Personal Data (hereinafter: the "Garante"). The obligation to notify in advance to the Garante processing of personal data has always been considered (especially by the Italian companies) a heavy obligation to comply with, even if, according to the original version of article 7 L. 675/1996:

> "Notification shall have to be given in advance and once only, by means of a registered letter or any other means suitable to certifying its receipt, regardless of the number of operations to be performed and of the duration of the processing, and may concern one or more processing operations for related purposes. A new notification shall only be made necessary by changes in the information provided and must be given before such changes are made."

And according to the successive article 26 L. 675/1996:

> "Processing and discontinuation of the processing of data relating to legal persons, bodies or associations shall not be subject to notification."

Article 7 of Law 675/1996 has been changed considerably (Link (in English) for the whole of the Italian law on Privacy 675/1996 can be found at: *www.privacy.it. Please note that this version does not include the corrective and supplementary rules as per Legislative Decree 467/2001*).

The principle is now that notification shall be compulsory only if the processing—taking into consideration its modalities and the kind of data involved—could be prejudicial to the data subject's rights and freedoms. This new general principle reverses the original general lines contained in article 7 about the notification to the Garante of the processing of personal data. In fact, the previous principles could be summarised in the following:

- A full and complete notification of the processing was the main obligation;
- A simplified notification could be carried out under certain circumstances (art. 7, paragraph 5-bis and 5-quater, now deleted);
- No notification was required in certain cases (art. 7, paragraph 5-ter, now deleted)

According to the new version of article 7 L. 675/1996, the general principle is now that the notification to the Garante is never required, except if the processing of personal data—taking into consideration its modalities and the kind of data involved—could be prejudicial to the data subject's rights and freedoms. The cases according to which the processing of personal data can be prejudicial (and the notification required) shall be specifically indicated by a successive Regulation adopted by a Presidential decree following a resolution of the Council of Ministers and with the consent of the Garante. It must be pointed out that said Regulation is already in force, but it needs to be amended taking into consideration the new provisions introduced by the Legislative Decree 467/2001 (Decree by the President of the Republic No. 501 of March 31, 1998: "*Rules on organisation and operation of the office of the Garante for the Protection of Personal Data pursuant to article 33(3) of Act no. 675 of December 31, 1996*". *Please note that the new provisions about the notification set forth in article 7 as amended by the Legislative Decree 467/2001 shall be effective from the entry into force of the amended Regulation*).

Information Provided When Collecting Data

The general principle contained in article 10 of L. 675/1996 is that the data subject as well as whoever is requested to provide personal data must be preliminarily informed, either orally or in writing, as to:

- the purposes and modalities of the processing for which the data are intended;
- the obligatory or voluntary nature of providing the requested data;
- the consequences if he fails to reply;
- the subjects or the categories of subjects to whom the data can be communicated and the area within which the data may be disseminated;
- the rights mentioned in the successive article 13;
- the name, denomination or trade name and the domicile, residence, or registered office of the controller and, when designated, of the processor.

The above information may not include those items that are already known to the subject where the data itself or knowledge of these items may hinder supervision or control by public bodies.

Additional information to be given to the data subject according to article 10 of the Law 675/96 have now been introduced by the Legislative Decree 467/2001:

- the name and address of the representative appointed in Italy by the controller of the processing settled in territories outside the EU;
- the name of at least one processor (whose appointment seems now to be compulsory and not optional according to article 8 of Law 675/96*);
- the indication of a telecommunication network site where a list of processors is made available to the public (this specific provision shall enter into force starting from March 1, 2002).

(**Article 8 (Processor):*

1. Where designated, the processor shall be a person having adequate knowledge, experience and reliability so as to ensure thorough compliance with the provisions in force applying to processing, as also related to security issues.

2. The processor shall abide by the instructions given by the controller in carrying out the aforementioned processing. The controller shall also verify periodically that the provisions (as per paragraph 1) and his own instructions are fully complied with.

3. If necessary on account of organisational needs, more than one person may be appointed as processor, even by subdividing the relevant tasks.

4. The tasks committed to the processor shall be detailed in writing.

5. The persons in charge of the processing shall have to process the personal data to which they have access by complying with the instructions given by the controller or processor.)

Consent to Processing of Personal Data

The general principle on which any processing is based is represented by the data subject's express consent (which must be given in writing with regard to the so-called sensitive data). In certain cases this consent is not required: article 12 of l. 675/1996 specifically indicates such cases (For the text in English of article 12 see: *www.privacy.it*).

The Legislative Decree 467/2001 has introduced a new case of exclusion of the data subject's consent to the processing: the data subject's consent shall not be requested and the processing of his personal data can be carried out in all the cases indicated by the Garante (according to the general principle of Law 675/1996) which states that the processing is based on a legitimate interest of the controller or of the third addressee of the personal data and the data subject's legitimate interests, rights, freedom and dignity do not prevail. The same new rule is introduced with regard to the cases of "communication" of personal data as per article 20 of the Law 675/1996.

According to article 1 of l. 675/1996 "communication" shall mean "the disclosure of personal data to one

or more identified subjects other than the data subject, in any form whatsoever, including by making available or searching such data". (For the text in English of article 20 see: *www.privacy.it*.)

Processing of "Sensitive" Data

Important provisions have been introduced with regard to the processing of sensitive data as per article 22 L. 675/96 (Sensitive Data) which provides:

> "Personal data allowing the disclosure of racial or ethnic origin, religious, philosophical or other beliefs, political opinions, membership of parties, trade unions, associations or organisations of a religious, philosophical, political or trade union character, as well as of health conditions and sex life may be processed only if the data subject gives his consent in writing, subject to authorisation by the Garante".

The particular conditions to legally carry out processing of sensitive data (written consent and authorisation by the Garante as compulsory, except the cases of General Authorisations given by the Garante to particular categories of Controllers) shall not apply when personal data related to the joining a Trade Union or labour union associations, confederations or organisations are processed. Further, processing of sensitive data shall be carried out on the basis of a simple authorisation given by the Garante (without the data subject's consent if necessary) when the processing is carried out by non-profit organisations, bodies, association of a political, religious, trade-union, philosophical nature (political parties and movements as well as religious communities included). The processing of personal data must have regard to the information of the supporters or the personal data of subjects which have regular contact with those associations, bodies, entities or organisations and must be licit. The communication or the diffusion of those personal data shall not be allowed if these processing (communication or diffusion) shall go beyond the scope and the activities of the organisations, entities or associations.

Further, processing of sensitive data shall be carried out on the basis of a simple authorisation given by the Garante (so without the data subject's consent as necessary) when the processing of sensitive data is necessary for carrying out the investigations referred to in Law of December 7, 2000 No. 397, or else for exercising or defending a right of a level equal to that of the data subject before a judicial authority, provided that the data are processed exclusively for said purposes and for no longer than is necessary. The Garante shall lay down the measures and safeguards referred to above and promote the adoption of a code of conduct.

New Category of "Particular Data"

The Legislative Decree 467/2001 introduces a new category of "particular data". Processing of personal data other than those mentioned in article 22 (sensitive data) and 24 (judicial data) of Law 675/96, but which present specific risks for the data subject's rights, fundamental freedoms and dignity, risks related to the kind of data involved, to the modalities of the processing and to the effects that the processing can determine, is allowed only on the basis of specific measures – when provided - which guarantee the data subject. These measures shall be indicated by the Garante on the basis of the general principles set forth by the Law 675/96 and according to a preliminary exam carried out by the Garante in advance upon a controller's request and relating to specific categories of controllers or processing (the specific acts to implement this provision shall have to be adopted within 120 days starting from October 1, 2002).

Transfers of Data to Third Countries

Simplifications have also been introduced by the Legislative Decree 467/2001 with regard to the transfers of sensitive or judicial data to third countries according to article 28 of law 675/1996. (For the text in English of article 28 see: *www.privacy.it*.) In fact, the general principle is now that the notification of a transfer is required only if the processing—taking into consideration its modalities and the kind of data involved—can be prejudicial to the data subject's rights and freedoms.

In any case, it must be pointed out that recently, in October 2001, the texts of new Authorisations for the transfer of personal data to third countries have been enacted by the Garante (see: *www.garanteprivacy.it/garante*):

- Authorisation for the Transfer of Personal Data to Switzerland
- Authorisation for the Transfer of Personal Data to Hungary
- Authorisation for the Transfer of Personal Data to Organisations Established in the United States of America in Compliance with the "Safe Harbor Privacy Principles
- Authorisation for the Transfer of Personal Data to Third Countries in Compliance with Standard Contractual Clauses.

The Sanctions

The Legislative Decree 467/2001 has introduced important modifications with regard to the system of sanctions set forth in the Law 675/1996. This system is characterised by the application—according to different hypothesis—of all the kinds of sanctions provided by the Italian Laws: criminal, civil and administrative sanctions.

According to the new provisions contained in the Legislative Decree 467/2001, the main crimes previously provided by the law 675/1996 and punished with the imprisonment (i.e.: article 34—Failure to notify or incorrect notification; and article 36—Failure to adopt measures required for data security) has been changed

into administrative illicit behaviours punished by administrative penalties. On the other hand (which may appear as a contradictory choice made by the Italian Legislator), a new crime—punished with the imprisonment from six months till three years—has been introduced. The new article 37-bis introduces the crime of Falsity in the declarations and notifications addressed to the Garante.

Furthermore, the administrative penalties have been increased: according to article 39 of Law 675/1996 the penalties provided a minimum of ITL 1,000,000 and a maximum of ITL 6,000,000. Now the penalties are: ITL 5,000,000—EUR 2,600 (minimum) and ITL 60,000,000—EUR 31,000 (maximum) and can be tripled taking into consideration the economic status of the transgressor.

It should be pointed out that in cases of committing the offence provided by the Law 675/1996, article 36 (Failure to adopt measures required for data security) the sanction of the two years imprisonment may be substituted by a penalty of from ITL 10,000,000 (EUR 5,164) to ITL 80,000,000 (EUR 41,000). Article 36 relating to the compulsory adoption (by January 1, 2001) of the security measures in the processing of personal data has been amended by the Legislative Decree 467/2001 introducing a sort of amnesty for those subjects who have still not complied with the obligations set forth in the Presidential Decree of July 28, 1999 No. 318 entitled: "*Regulations including provisions for laying down the minimum security measures applying to the processing of personal data in pursuance of Article 15(2) of Act no. 675 of December 31, 1996*".

In summary, the failure to adopt measures required for data security is always considered a crime, but a term (not exceeding the period technically necessary and in any case not superior to six months) can be fixed for the guilty subject in order to regularise his position by means of the adoption of the compulsory security measures. In the sixty days successive to the expiration of the mentioned term, if the subject has adopted the proper and requested measures, the crime shall be extinguished by paying a penalty.

Codes of Conduct

The Legislative Decree 467/2001 provides that the Guarantee shall promote by June 30, 2002 the adoption of Codes of Conduct with regard the processing of personal data in the following fields:

- telecommunication and telematic services sector;
- marketing and advertising, market research and interactive commercial communications sector;
- employment sector;
- credit to the consumers sector;
- video surveillance carried out by private or public subjects;
- management by public subjects of data banks, registers, lists.

The adoption and the respect of these Codes of Conduct shall be a necessary pre-requisite of a licit processing of personal data.

The provisions about the adoption of Codes of Conduct develop the "promotional" aspect of the Law 675/1996 as an act containing general provisions to be in any case specified (according to the particular needs of protection) by sectorial Codes of Conduct enacted by the interested categories.

Protection of Privacy in the Telecommunication Field

Finally, The Legislative Decree 467/2001 has also introduced non-relevant modifications to the Legislative Decree of May 13, 1998 No. 171 "*Implementation of the EU Directive 97/7/EC related to the protection of the privacy in the Telecommunication field*".

It is now provided (starting from February 1, 2002) that publicly available telecommunication services providers must make available for consumers modalities of payments alternative to the invoicing (i.e.: pre-paid cards). This was an optional provision before. Further, they must document and send by June 30, 2002 to the Guarantee all the measures set up to allow these alternative modalities of payments. The violation of this provision shall be sanctioned with an administrative penalty from ITL 5,000,000 (EUR 2,600) to ITL 30,000,000 (EUR 15,500) which can be tripled according to the economic status of the transgressor. If the measures adopted are deemed insufficient by the Garante, the Garante shall indicate it to the controllers or shall prohibit the processing.

With regard to the identification of the calling line, publicly available telecommunication services providers or public telecommunication service providers must inform the consumers more specifically about the existence of this service.

Finally, with regard to the emergency calls it is provided that publicly available telecommunication services providers or public telecommunication service providers must adopt proper and clear measures to guarantee, telephonic line by telephonic line, the deletion of the service of identification's cancellation.

SPAIN

New Electronic Signature Act Draft

By Almudena Arpón de Mendívil of Gomez Acebo & Pombo at www.gomezacebo-pombo.com. E-mail: Aam@gomezacebo-pombo.com. First published in "the l.i.n.k." (a free bi-monthly electronic newsletter on Information Society legal issues, edited by Le_Goueff@vocats.com.

Introduction

The Spanish Ministry of science and technology has published on its official website the first draft of the new Electronic Signature Act (hereinafter, referred to as "the Draft"), which will substitute current regulations included in Royal Decree 14/1999. Before being submitted to the Spanish Parliament, the Draft was made available for public consultation during January 2002. Any comments on the Draft should be sent to the following e-mail address anteproyecto.firma@setsi.mcyt.es.

Pre-existing Situation

Legislation on electronic signature in Spain was formed by Royal Decree-Law 14/1999 of September 17, approved early on, even before EC Directive 1999/93 of December 13.

The Draft reinforces the legal framework for the electronic utilisation of firms and the legal regime of the services of certification, extending the regulation to distinct aspects of the relations based on the use of certificates and electronic firms that the Real Decree-Law 14/1999 did not outline, due to the urgency of its approval before the referred EC Directive.

In this respect, the Draft precisely determines the minimum requirements to carry out activities related to certification of electronic signature and also the due diligence and responsibility for the providers of certificates.

Main Aspects

The main aspects of the Draft are as follows:

- the consideration of the electronic signature equivalent to the regular signature under certain conditions indicated in the Draft for private transactions but also for relations with the public administration;
- to give an electronic signature the same legal consequences as a regular signature according to the already existing civil and litigation Spanish laws in force;
- to create a personal electronic signature not only for the individuals but also for companies;
- to create a new electronic Spanish National Identity Card for electronic identification of Spanish citizens; and
- to regulate the certification services to be provided by private and public entities (incorporated in Spain or having permanent presence in Spain) and their responsibilities and compulsory insurance.

Electronic Signature vs. Advanced Electronic Signature

The Draft maintains the distinction created under Royal Decree 14/1999 between the "electronic signature" and the "advanced electronic signature", the difference being that the second allows the identification of the individual or company who signs, and has been created under systems that the signatory can maintain under his or its exclusive control and exclusively related to him, allowing any modification of the elements and data incorporated into the signature to be detected.

Certificate vs. Recognised Certificate

There is also an important distinction between the terms "certificate" and "recognised certificate" which basically refers to the number of elements that are included in order to make identification of the signatory and his identity more accurate and give them greater precision.

For that purpose, the recognised certificate must include the following information:

- reference that it is issued as a recognised certificate;
- the unique identity code of the certificate;
- the identification of the certificate services provider and its business address;
- the advanced electronic signature of the certificate services provider;
- the identification of the signatory by his name and surnames or by pseudonym or company's name or other personal identification elements;
- the data, codes or cryptographic clues under the control of the signatory;
- the period of validity of the certificate;
- the general limits on issuing the electronic signature if applicable; and
- the amount limits on issuing the electronic signature if applicable.

Providers of Electronic Certificates

The providers of recognised certificates are obliged to assume extra obligations fundamentally referred to its human and technical organisation.

Any provider of certificates is liable for all damages caused to any individual or company due to the breach of its obligations under the Draft, as it is they, and not the individual or company, who are obliged to prove

that they have acted under the provisions of the Draft with the necessary due diligence.

The Draft also includes a list in order to limit the liability of the providers under extraordinary circumstances or under a previous breach of other provisions of the Draft by the signatory or any third party.

The providers of recognised certificates also have to subscribe a guarantee of no less than EUR 6,000,000 in order to cover possible liabilities arising by breach of the provisions included in the Draft.

The certification services to be provided by the providers are not subject to any special condition but special mention is made by the Draft to a future voluntary certification and accreditation system to be developed by the Ministry of Science and Technology, which will also include the conditions to be fulfilled by the entities that will certify the validity of the providers to carry out their activity.

The Draft also includes some provisions referring to the software used to create and verify the data incorporated into an electronic signature, which shall fulfil the resolutions issued by the EU or Spanish authorities in the near future.

Administrative Control

Control over providers and services is reserved for the Ministry of Science and Technology together with the Spanish Data Protection Agency with reference to the protection data matters.

Nevertheless, the Ministry of Justice will be in charge of the Register to record the identity of all service certification providers to be created in further developments of the Draft after its approval by Parliament.

Infringements and Penalties

Finally, the Draft includes a provision referring to infringements and penalties for breach of the provisions of the Draft, together with the possibility of adopting interim measures by the administration under certain extraordinary circumstances.

GERMANY

Internet Data Protection to Become Easier

By Dr. Kai von Lewinski and Dr. Marcus Schreibauer, lawyers in the Frankfurt and Düsseldorf offices respectively of the law firm Lovells Boesebeck Droste.

Amendments to the Teleservices Data Protection Act in Germany will make it more practical.

Up until now many companies have ignored the legal requirements governing the protection of personal data on the internet. One of the main reasons for this was that some provisions of the Teleservices Data Protection Act (Teledienstedatenschutzgesetz, TDDSG) imposed unreasonable requirements on internet service providers. The amended TDDSG, which is due come into force at the beginning of this year, should have the effect of making data protection in the internet easier. At the same time, fines will be imposed for the first time under the new regulations on those providers who fail to comply with certain of these requirements.

Collecting personal data is particularly important in the internet industry. Online-shops are particularly interested in collecting data relating to the purchasing behaviour, or other special interests, of their customers and in processing such data for marketing purposes. Since it is possible to collect an extensive amount of data by means of a number of software tools, the TDDSG was enacted in 1997 in order to control the use of personal data on the internet and thereby prevent data misuse. Soon after the TDDSG came into force however, people in the internet industry and data protection experts pointed out various problems with the TDDSG, which are now being addressed by the amendments.

Scope of Application Clarified

Due to the wide interpretation of the wording of the TDDSG, the scope of application of the TDDSG immediately became a controversial issue. The amended provisions have been drafted more clearly and, in particular, now state that the TDDSG does not apply to data processing within or between companies or public authorities where the internet services are used exclusively for the control of work flow and business processes. As per the government's intention, distribution data or management information systems, for example, will not be affected by the restrictions of the TDDSG.

Under the TDDSG, it was possible to create so-called "pseudonym" user profiles, namely the replacement of a user name by a number, for example, but up until now the authorised scope of use of these user profiles has been a matter of widespread debate. The amended provisions now make it clear that "pseudonym" user profiles may be used for advertising, market research and for structuring telecommunications services. For data processors this is a positive step towards identifying what they are allowed to do.

Methods for processing accounting data have also been increased. Accounting data from various services can in future be brought together, thus allowing the services to be invoiced more efficiently. Furthermore, service providers will now be able to pass on their accounting data to debt collection agencies, which do not provide internet services themselves. In addition, the provider will now be able, under certain circumstances, to process data without the user's prior consent if this assists in uncovering abuses of the internet services.

The current version of the TDDSG contains a particularly impractical provision relating to the electronic consent given by the consumer in relation to the use of his or her data. Under German law, this consent is required for many direct marketing methods on the internet but as yet, it can only really be granted by means of a digital signature, which is not yet in widespread use.

Consent Under Amended Provisions

Under the amended provisions of the TDDSG, consent will be effective if:

- it is given by means of an unambiguous and deliberate act on the part of the user;
- the content of the consent is recorded; and
- it can be withdrawn by the user at any time.

It will now be possible, for example, for the consumer to give its consent by clicking a button on the relevant web site. Valid consent does require, however, that the consumer is fully informed of the purpose and extent to which its data is used. A hidden or slightly obscure reference, as is often found in the general terms and conditions of many internet businesses, will not be sufficient. In accordance with the transparency requirements of the data protection laws, the less the intended use of the data is to be expected by the user, the clearer the reference to it must be.

Liability for Breaches

If the provider breaches certain obligations (for example the requirement to inform the user about details of data use, or the obligation not to combine a user profile with data concerning the bearer of the pseudonym), it will be liable, under the amended TDDSG, for a fine of up to DEM 100,000. The data protection supervisory authorities have already said that they will focus on the on-line sector with the result that breaches of the TDDSG will be met not only with warnings from competitors but also fines and prohibitory injunctions. Against this background, on-line companies are well advised to implement the new legal provisions as soon as possible, particularly because consumer trust in its own on-line offering can only be strengthened through a clear and reasonable privacy policy.

INTERNATIONAL DEVELOPMENTS

■ CYBERCRIME

New Cybercrime Plans for Australia Similar To Europe

Controversy continues to surround new cybercrime laws that have been adopted in various parts of the globe.

In Australia, the Federal government has approved a Cybercrime Act that will greatly expand the power of government agents to conduct surveillance along computer networks. It will require Internet users to hand over their private encryption keys, and criminalises several types of online activity, such as impairment of electronic communications. Greg Taylor from Electronic Frontiers Australia (EFA-a GILC member) warned that the law could have an adverse effect on innocent behaviour, and that his organisation had "major concerns about gung-ho prosecutions based on insufficient knowledge on the part of law enforcement agencies."

The measure bears certain similarities with a Council of Europe (CoE) Cybercrime Convention that was recently signed by representatives from 30 nations, including Japan, South Africa and the United States. Among other things, the Convention would require countries to authorise government agents to install spytools on the servers of Internet service providers (ISPs) and thereby intercept all Internet transmissions that come through the servers. The treaty requires signatory nations to comply with foreign investigators, even when they are investigating activities that are not crimes on domestic soil. The CoE pact has received harsh criticism from many quarters, including privacy advocates and business groups. The treaty will now be sent to certain individual states for ratification.

For more on the Australian cybercrime proposal, read Simon Hayes, "Lobbyists slam cybercrime laws", December 21, 2001 at *http://australianit.news.com.au/articles/0,7204,3476612%5E15306%5E%5Enbv%5E,00.html.*

The final text of the Council of Europe Cybercrime Convention is available via *http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185&CM=8&DF=11/01/02.*

See "European Union Holds Cybercrime Conference-Update", Newsbytes, November 27, 2001 at *www.newsbytes.com/news/01/172449.html*

Read Denes Albert, "Bad News for Hackers," Reuters, November 21, 2001 at *www.cbsnews.com/now/story/0,1597,318911-412,00.shtml*

■ CONSUMER PROTECTION

Internet Sweep to Seek Cyber Health Scams

Consumer and health protection authorities from 30 countries—including the U.S. and Australia—will search thousands of websites to uncover deceptive, false or misleading health claims, according to a January 20, 2002 announcement by the Australian Competition and Consumer Commission (ACCC).

The International Marketing Supervision Network (IMSN) Internet Sweep is targeting websites that offer "miracle" health products and services as well as sites promoting legitimate products as if they have properties they do not have, the ACCC reported.

The growth of the Internet has precipitated increased cross-border consumer transactions that bring law enforcement changes for authorities.

In addition to being an active player in the IMSN, the ACCC is the International Sweep Day Coordinator and will be assuming the presidency in the next financial year.

ACCC Chairman Allan Fels remarked:

> "While the advent and proliferation of the Internet had been valuable for societies around the world, there are unscrupulous business people who are using the medium to make a fast dollar by taking advantage of vulnerable consumers. … Health shams not only waste consumers' money, but in extreme cases may harm their well being."

Instead of focusing on policy discussion like the OECD Committee on Consumer Protection, the IMSN is based on action, the ACCC noted. The Sweep Day, it added, is a significant annual event on the IMSN calendar.

The IMSN is a network of consumer protection authorities of 30 countries, whose main objective is to take action to prevent and redress deceptive marketing practices. The group has an international component and fosters cooperative efforts by member authorities to tackle consumer problems connected with cross-border transactions in both goods and services. Information exchanges between member authorities also play a key role in effective investigations and court action where necessary.

The 30 IMSN Member Countries are Australia, Belgium, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Republic of Korea, Latvia, Luxembourg, Latvia, Mexico, The Netherlands, New Zealand, Norway, Poland, Portugal, Slovak Republic, Spain, Sweden, Switzerland (current President), the U.K. and the U.S.