the 23rd International Conference of Data Protection Commissioners
Paris, 24/25/26 september 2001

le Journal

of the 23rd International conference of Data Protection Commissionners

National Data Processing and Liberties Commission / France

April 2001 / # 2

FOCUS

The powers of sanction of the Spanish data protection agency :

A real 'a posteriori' control of files. Fines from 601€ to 601,000 €. **Page 2**

THE STAKES

Is it really possible to carry out an independent control of police files? :

Schengen, Europol, the European experience. **Page 3**

Who is reading your e-mail?

TOPICALITY

Monitoring of e-mail and internet access at work is a hot topic in the UK.

by Elizabeth France
Information Commissioner - UK

" Employers' new powers to spy on your e-mails could cost you your job " is typical of the newspaper headlines. This misleading information has led to widespread uncertainty as to the limits of employers' powers.

UK law has historically treated the unauthorized interception of communications on a public network as a criminal offence, but until recently it has not specifically addressed interception on private networks, such as those in most workplaces. The EU "Personal Data Protection and Telecommunications" Directive and the European Convention on Human Rights have changed this situation. **The Regulation of Investigatory Powers Act of October 2000** makes such interception unlawful, except in case of consent or where the interception is in the framework of "lawful business practice". Such practices are defined in separate regulations but are wide and include monitoring, both to ascertain compliance with business standards, and to detect unauthorized use. The publication of these regulations generated misleading headlines and led employers to believe that there were few, if any, restrictions on their powers to monitor e-mail and internet access.

The new law does no more than, for the first time, establish a clear, lawful basis for interception. Such interception, which involves the obtaining of personal data, the storage and the subsequent use of those data, remains subject to the requirements of general data protection law.

However, monitoring does not necessarily require interception. It may, for example, be based on the examination of e-mail messages that have already been received, opened and then stored by the addressee.

The Code of Practice on the Use of Personal Data in Employer/Employee Relationships

So, what impact does the RIP Act have on data protection, monitoring of e-mail and internet access in the workplace? This is where our draft Code of Practice comes in. Any monitoring must be a proportionate response by the employer to the risks he faces. In giving practical guidance on what is meant by a proportionate response, the draft Code proposes standards that employers must comply with.

The Standards proposed by the Code

Establish the specific business purpose for which monitoring is to be introduced.

Assess the impact of monitoring, not only on the rights of freedom of staff, but also on others, such as recipients,

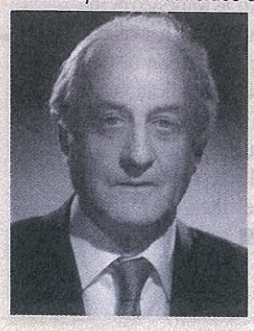
continued on page 2, col.2

EDITORIAL

by Michel Gentot
President of the National Data Processing and Liberties Commission

Yahoo, Toysmart etc.

The call to order pronounced by a French judge concerning an auction website, with an address in the United States, who put up for sale Nazi emblems, whose distribution is prohibited in France, and the refusal by the United States that a file of clients of a bankrupt company might be considered an element of asset, and therefore tradable, have two points in common : the internet and the judge. These confrontations, which are not unprecedented in any of our countries, have, however, had worldwide repercussions that a paradox, one which is at least obvious, has only exacerbated. So, the "national law" of a country of freedom is supposed to be able oppose the network of worldwide distribution? So, personal data protection is supposed to be assured - and how! - in the United States? These questions remain open on both sides of the Atlantic.



The recent discussions I have had with the legal authorities of the State of New York, during a visit to the United States, have convinced me of the need to open this debate during the Paris Conference, because there is no longer any decision related to the internet that does not concern all the citizens of the world.

Who is reading your e-mail?

continued from page 1

senders, and those referred to in messages.

Remember that business messages may also contain private information.

Determine whether the business purpose can reasonably be achieved in other, less intrusive ways.

Do not introduce monitoring where the adverse impact is out of proportion with the benefits.

Target monitoring on areas of particular risk.

Restrict monitoring, as far as possible, to traffic rather than content of messages.

Use automated monitoring so as to reduce the extent to which personal information is revealed.

Avoid opening messages that are clearly of a personal rather than business nature.

Make all staff, subject to monitoring, aware of its taking place and the purpose for which personal information is collected.

Do not use personal information collected through monitoring for other purposes, unless an employer could not reasonably ignore it.

Our draft Code addresses many issues other than monitoring, but this is the subject that has attracted by far the most interest. We are now analyzing over 100 responses received to the public consultation. Many are hostile to our proposals on monitoring. We shall take account of the views expressed, hold further discussions, and then publish a final version of the Code. The challenge is to translate this general proposition, with which few would disagree, into clear, workable standards for employers. ■

INTERVIEW

Malcom Crompton - Australia

Federal Privacy Commissioner since April 20, 1999 and responsible for applying the Privacy Act 1988.

What is the objective of the new Privacy Act, and the new rights, which comes into force on December 21, 2001?

The new legislation of December 6, 2000, which is an amendment to the 1988 Privacy Act, concerns private sector organizations. These must act according to the National Privacy Principles, which in turn are based on the OECD Guidelines.

For the first time, this law allows individuals the right to know the reasons for which private sector organization collects their personal information, what data it holds (and the right to correct any wrong information), what use will be made of the data, and who else might obtain them. Consumers may make a complaint to the Privacy Commissioner or apply to Federal jurisdictions for an order instructing organizations to correct their practices to make these consistent with National Privacy Principles.

To whom will the new private sector provisions apply?

The Act will apply to organizations in the private sector, including charitable organizations, sports clubs and unions, with a turnover of more than $3 million, federal government contractors, health service providers, and organizations who deal in personal data (whatever their turnover). The Act is also optionally applied to small businesses who choose to submit to the new legislation.*

Who is not covered by the new provisions?

The Act does not over political parties, most small businesses with an annual turnover of less than $3 million, data collected in the framework of normal personnel management, and media organizations in the practice of journalism.

What are the innovations provided for in the Act?

The Act encourages organizations to adopt their own code of deontology which must be approved by the Privacy Commissioner. This approval can only be granted if the code is, at least, equivalent to the National Privacy Principles. The code may specify an independent data protection adjudicator to handle complaints. If the code does not make such a provision, the Privacy Commissioner is the default code adjudicator. Organizations that do not have their own code must comply with the principles set out in the Act. We are actively working with the private sector to promote good privacy practices and to encourage adoption of codes of deontology. I very much look forward to sharing your experience in Paris and, in the meantime, invite you to consult our website, www.privacy.gov.au.

**3 million Australian Dollars = 1 737 918 euros*

The powers of sanction of the spanish data protection agency

FOCUS A real 'a posteriori' control of files: the experience of the Spanish authority

Par Juan Manuel Fernández López ,
Director of the Data Protection Agency - Spain

Fines from 601€ to 601,000 €

The Spanish legislature has given the Data Protection Agency the power to impose penalties ranging from 601 € to 601,000 € according to the gravity of the infraction committed, to order data processing to be ceased as well as the pure and simple destruction of any files which do not comply with legal provisions.

Its powers must be exercised only as a last resort.

Inspections by sector of activity are carried out each year in order to make those responsible for the files aware of their obligations. Following these inspections the Agency issues targeted recommendations which are widely distributed in the sectors concerned. A sanction procedure is started only in the cases where serious infractions are noted.

In the year 2000 the sectors aimed at were e-business files, the large stores' customer loyalty cards, and mobile 'phones. The Agency imposed a total of 11,293,000 € in penalties, the most sanctioned sectors being the internet, telephones, patrimonial solvency, credit, and health.

But sanction is not everything!

The Spanish law is increasingly well known, as witnessed by the considerable growth in all our activities: declaration of files (registration, modification and deletion) +500%, number of cases brought by individuals + 40%, and access to our website (more than 1 million) +132%. ■

An independent control of police files: Schengen, Europol, the European experience

THE STAKES Is it really possible to carry out an independent control of police files? That is the question which many citizens in each of our countries ask themselves.

Alex Türk,
Senator, Member of the CNIL (F) and President of the Europol Joint Supervisory Body, evokes the European experience.

Police co-operation in Europe is principally based on two main files. The Schengen information system concerns, essentially, individuals wanted by the police and foreigners having been expelled from the 'Schengen space'. The Europol files concern important international crimes (drugs trade, terrorism, etc.) and comprise, not only an index, but also files of analysis.

The recognition of a genuine legal base of guarantees

The fear which appeared at the end of the 1980s, during the first discussions concerning the setting up of European police files, was that these files might escape each of the national data protection laws of the European Union countries. Luckily, the national data protection authorities were able to make the European governments accept that the conventions setting up these files should comprise personal data protection measures.

A right of access which must be exercised

When it concerns the Schengen system, the right of access is exercised according to national applicable law in the country where the request is lodged. In France it is exercised through the CNIL. In the year 2000 the CNIL received nearly 400 requests for right of access, which in 30% of the cases led to the suppression of any 'Schengen file'.

On the other hand, for the moment very few requests for right of access to Europol files have been made. The Europol Convention, however, comprises a major innovation: the setting up of a real appeals committee, an independent authority charged with examining the complaints lodged by individuals who are not satisfied by the response - or the absence of response! - to their request for right of access.

An independent supervisory body

In both cases, an independent joint supervisory body, exclusively composed of national data protection authority representatives, is charged with checking the functioning of the implemented files.

The Schengen joint supervisory body has, thus, carried out four controls of the central system, installed in Strasbourg, which have led it to recommend that security measures be strengthened.

The Europol joint supervisory body has even wider powers. It ensures the on site control of the functioning of the files (the first one took place in November, 2000). Furthermore, it is charged with giving its advice on any new file creation. Finally, the assignment of the appeals committee, chaired by our colleague, Peter Hustinx, is to investigate the complaints made by individuals who are not satisfied by the response received to their request for right of access.

Independence to be strengthened and information campaigns to be carried out

It is given, that independence cannot be acquired in one day. It is needless to remind anyone of the action led in these matters by Bart de Schutter, President of the Schengen Joint Supervisory Body, despite the fact that the authority still does not dispose of an independent budget.

Finally, the joint supervisory bodies are working at making themselves better known through information campaigns. The Schengen joint supervisory body has set the example by distributing brochures describing the purpose of the file and the right of access, at borders and airports.

The imperative of public order and the protection of personal data should not be incompatible: this is the European conviction! ■

TODAY'S FIGURE

10 Thousand Million Euros

The annual cost to internauts of unsolicited messages or "junk mail"

Source: European Commission.

NEWS IN BRIEF

UNITED KINGDOM

Freedom of Information Act 2000 - UK. As of January 31, 2001, Elizabeth France and her Services are charged with enforcing not only the Data Protection Act 1998, but also the Freedom of Information Act 2000.

HONG KONG

"Something for everyone" during the Privacy Week in Hong Kong from March 26 to April 1, 2001. Our dynamic colleague, Stephen Lau, the Hong Kong Privacy Commissioner for Personal Data (PCO-Privacy Commissioner's Office), organized a Privacy Week to coincide with the Asian Data Privacy Forum and which included: a conference on E-Privacy in the New Economy, a TV Privacy Night show, a student competition of the best designed website for raising awareness of the importance of personal data protection and privacy in their peer groups, two seminars on the PCO's new Code of Practice for human resource management, and finally, a road show crossing Hong Kong on March 28 and 31, and April 1. Bravo!

NEWS IN BRIEF

UNITED STATES
Legal decisions - **What contents for the future Federal Law?** At the beginning of March the Committee on Energy and Commerce of the House of Representatives started their hearings on privacy issues. Stefano Rodotà, Chairman of the European Data Protection Commissioners' Group, set up by Directive 95/46/CE, testified on March 8.

On January 11, Eliot Spitzer, Attorney General of the New York State, who objected as 43 other states and the Federal Trade Commission, to the online children's toy store "Toysmart"'s plan the sell costumer list while beeing in bancruptcy, annouced the Bankrupcy Court in Boston's settelment . The agreement says Walt Disney Company will pay 50 000 US $ to its subsidiary Toysmart to destroy the list. Accordine to the Assistant Attorney General interviwed by CNIL, the intention of selling the list, not beeing part of its privacy policy at the time of collection of the data, would have constituted a "deceptive practice" , and would have been unlawfull, without the parents' consent of the concerned children under the Children's Online Privacy Act of 1998.

According to 'Financial Times' of February 27, 2001, 300 privacy related bills are under consideration in various states and at least a dozen at the Federal level.

ERRATA
Two errors appeared in our first issue: our colleague, Dr Ewa Kulesza, is a specialist in Labour Law and Social Sciences, and the exact spelling of our New Zealand colleague's name is Bruce H. Slane. With our humble excuses.

Paris Conference

When ?
September 23 to 26, 2001

How ?
You can register right now by completing the attached form or, of course, on our website **paris-conference-2001.org**

Attn! - it is very difficult to get a hotel room in Paris in September, book a.s.a.p.!

le Journal

Le Journal is published by the Commission Nationale de l'Informatique et des Libertés, France.
Director of publication, Michel Gentot.

Création Salvador

Please send your reactions and contributions to:
Michel GENTOT
mgentot@cnil.fr
Thierry JARLET
tjarlet@cnil.fr
Marie GEORGES
mgeorges@cnil.fr

The "Berlin Group"

WORKING GROUP

An International Working Group on Data Protection in Telecommunications

Hansjürgen Gartska,
Data Protection and Information Access Commissioner of the State of Berlin - Germany

The Background
In 1983 the former Data Protection Commissioner of the State of Berlin, Germany, Dr Hans-Joachim Kerkau, invited all then existing Data Protection Authorities to attend the International Audio and Video Fair in Berlin, where the latest products of the telecommunications industry were exhibited, particularly the videotext and cable television technologies. The colleagues, invited to participate in a workshop, prepared a resolution on problems of data protection in these areas. This was adopted by the International Conference of Data Protection Commissioners in Stockholm on October 18, 1983. The Conference had already stated that "personal data which are automatically collected... can be used to draw up individual profiles of all users. Users' social relations and patterns of behaviour can in this way be made the object of other measures".

The group soon called itself the "International Working Group on Telecommunications and Media". During the 11th International Conference in Berlin in August 1989 it was decided, on the proposal of the French delegation, to extend the activities of the working group, which from then on met twice a year, the Spring meetings being held in other countries, including the USA, Russia, Hong Kong, and India.

Due to the informal nature of the working group, the International Conference decided, in Manchester, 1993, to adopt no more resolutions submitted by the working group, but reports on its work have been given by every Conference since then.

Working Group Reports

Luxembourg, 1985 - The Impact that the Development of New Electronic Media, Cable Networks, and the Digitalization of Telecommunications Services could have on Users' Privacy.

Sydney, 1992 - Problems relating to the Secrecy of Telecommunications and Satellite Communications, where positioning and fleet management systems as well as remote sensing are discussed.

Berlin, 1996 - Data Protection and Privacy on the Internet (the " Budapest-Berlin Memorandum "), which deals with the insufficient legal and technical protection of Internet users' privacy and proposes measures to improve this.

Hong Kong, 1998 - Search Engines on the Internet, where the capability of search engines to produce profiles of people's activities on the Internet is discussed, and recommendations for more privacy-friendly practices are made.
Public Accountability in Relation to Interception of Private Communications, which stresses the importance of mechanisms to re-assure the public that interception powers are being used lawfully, appropriately, and proportionately.

Norway, 1999 - Privacy Risks Associated with the Use of Intelligent Software Agents, which calls on system designers to incorporate measures to protect privacy in their products, i.e. Privacy Enhancing Technologies (PET), in particular for authentification of all agents, access control mechanisms and tools to give a user control over third parties' agents.

Crete, 2000 - The Processing of Personal Data for the Detection of Fraud in Telecommunications , where the Group discusses various types of fraud detection and prevention methods regarding privacy impact.
Privacy and Copyright Management (Crete, 2000) gives recommendations on the design and use of Electronic Copyright Management Systems (ECMS) to strike a fair balance between copyright holders and users' privacy.

Berlin, 2000 - Data Protection Aspects in the Council of Europe Draft Convention on Cyber-Crime , where, in particular, the Group explicitly refuses proposals to oblige telecommunications and Internet service providers to store data on all telecommunications and Internet traffic for an extended period, in order to have the data to hand should a crime occur during this period.

Bangalore, India, February 2001 - Mobile Location, principles for the privacy friendly design and operation of the location of information based services.

Future Projects
The 30th meeting will take place in connection with this year's International Audio and Video Fair in Berlin on August 27-28, under the title "Privacy and Intellectual Property Rights on the Internet". ■

Documentation:
www.datenschutzberlin.de