BNA International

World Data Protection Report

International Information for International Businesses

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

Volume 7, Number 2 February 2007

Articles

Personal Data

Italy: Recent Developments in Data Protection – Guidelines on the Processing of Employee Personal Data by Employers Within the Private Sector 3

Security & Surveillance

The Golden Rule of Privacy: A Proposal for a Global Privacy Policy On Government-to-Government Sharing of Personal Information 13

Legislation and Guidance

Binding Corporate Rules: An Honest Appraisal from the U.K. Information Commissioner's Office 21

Data Protection and Intellectual Property: Document Number 104 from the Article 29 Working Party 24

UK Government Announces Tougher Penalties for Data Protection Offences 10

News

Personal Data

Inquiry Reports Can Include Confidential Records 7

Stop Press: Express Obligations of Confidentiality Affect Privacy Rights 8

The Impact of McKennitt v Ash – English Court Extends the Protection of Privacy and Confidential Information 8

Security & Surveillance

Belgium – Privacy Commission Considers Whistle-blowing Hotlines 16

Legislation & Guidance

Irish Privacy Law Poses Threat to Press Freedom 28

Obligations Under Franchise Agreement and Data Processing Requirements – Alleged Conflict 11

Online Shopping Under the E.U. Microscope 11

www.bnai.com

BNA International Inc., a subsidiary of The Bureau of National Affairs, Inc., Washington, D.C., U.S.A.

Publishing Director: **Deborah Hicks**
Editorial Director: **Joel Kolko**

Editor: **Jeremy Kuper**

Production Manager: **Nitesh Vaghadia**

Submissions by Authors: The editors of *World Data Protection Report* invite readers to submit for publication articles that address issues arising out of the regulation of data protection, either on a national or transnational level. Articles with an appeal to an international audience are most welcomed. Prospective authors should contact Nichola J.L. Billington, World Data Protection Report, BNA International Inc, 29th Floor, Millbank Tower, 21-24 Millbank, London SW1P 4QP, U.K. Tel. (+44) (0)20 7559 4807; fax (+44) (0)20 7559 4880; or e-mail: nicholab@bna.com. If submitting an article by mail please include an electronic copy of the article in a recognised software.

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: 29th Floor, Millbank Tower, 21-24 Millbank, London SW1P 4QP, England. Tel. (+44) (0)20 7559 4801; Fax (+44) (0)20 7559 4840; e-mail marketing@bnai.com. In the U.S. call toll-free on: 1-800-727-3116.

Subscription price: U.K. and rest of world £695; Eurozone €1,125; U.S. and Canada U.S.$1,195. 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.

Website: *www.bnai.com*
ISSN 1473-3579

Dear readers, as you are well aware, the primary focus of this journal is to review developments in privacy law internationally. Privacy and data protection legislation has been introduced, or updated in most jurisdictions in the past decade, and it is my aim as editor in this fast changing legal landscape, to keep practitioners constantly updated in relation to changes wherever they may occur.

Privacy laws have been used as a way of protecting IP, such as in the recent McKennitt v Ash case in the United Kingdom, which is considered in depth by Jean-Michel Jost of the law firm Bird & Bird. Ian De Freitas partner with the firm Berwin Leighton Paisner LLP summarizes the U.K. position very well in relation to recent case law involving celebrities from Naomi Campbell, to Michael Douglas, not forgetting H.R.H Prince Charles.

These changes in the U.K. have in turn led to interesting developments in relation to the interaction of privacy law with IP regimes. There is now even a question amongst some experts, of whether a right to privacy can itself be considered to be a property right. It is already considered to be a 'personality right' in certain E.U. jurisdictions.

There is also an in-depth look at possible data sharing between the U.S. and E.U. in this issue by John Kropf from the U.S. Department of Homeland Security.

Additionally, new developments in the area of Digital Rights Managements Systems (or DRM's) demonstrate that this is a subject of growing importance, and I have included several articles looking at the current legal questions arising from the increased use of DRM's. There is so much to tell you, I think you will just have to read it for yourselves and judge...

We wish to thank the following for their contribution to this issue:
John Kropf, U.S. Department of Homeland Security, Washington D.C.; *Boris Wojtan,* Information Commissioner's Office, Cheshire; *Alessandro Del Ninno,* Studio Legale Tonucci & Partners, Rome; *Sylvie Rousseau,* Linklaters, Brussels; *Jean-Michel Jost,* Bird & Bird, London; *Gary Brooks, Ian De Freitas & Vanessa Barnett* of Berwin Leighton Paisner LLP, London; *Leonardo Cervera Navas,* European Commission, Brussels; *Andrew Clay,* Hammonds, Leeds; *Dr Chris Pounder,* Pinsent Masons, London

Personal Data

Italy: Recent developments in Data Protection – Guidelines on the processing of employee personal data by employers within the private sector.

By Avv. Alessandro del Ninno, Information & Communication Technology Department, Studio Legale Tonucci & Partners, Rome. The author may be contacted at adelninno@tonucci.it.

On December 13, 2006 the Italian Data Protection Authority (hereinafter the "*Garante*") made public the guidelines on the processing of employees' personal data for labour relationship management purposes by employers within the private sector' (the "guidelines"). For the first time, the Italian *Garante* has defined – within a global and co-ordinated framework – rules and guarantees aimed at regulating the gathering and the processing of personal data within the work-place. The guidelines can also be interpreted as a practical set of rules executing the general principles contained – on this specific subject matter – in the related provisions of the Italian Code on privacy (legislative decree of June 30, 2003 no. 196). It is worth noting that in the coming weeks the Italian *Garante* shall hold discussions aimed at clarifying certain specific issues. The *Garante* has announced that the next set of guidelines shall consider the processing of the employees' personal data, within their use of e-mail and Internet connections from the workplace. The guidelines also set out principles and rules applicable to employers and employees within the private sector. With regard to the public sector the rules are different, and in any case these guidelines are focused on private employers and employees.

§ 1. Processing employee personal data: the general scopes considered by the guidelines.

The principal issues taken into consideration by the guidelines mainly refer to the following aspects of the processing of employee personal data:

a. employee personal and generic data (with no regard as to whether the employee is not working any more), biometric data, pictures and sensitive data (also when referring to third parties) with particular regard to data allowing the disclosure of religious beliefs or memberships to trade unions;

b. employee personal data disclosing health (usually contained in medical certificates, or in other documents delivered by the employee to the employer for justifying absence from work or to get permits and benefits provided by the laws or by the collective agreements);

c. information more closely related to the carrying out of the work activities, for example: information related to the kind of contract (whether temporary or permanent, full time or part-time, etc.), information relating to the employee's professional level or title, to his salary (even when calculated "*ad personam*"), to prizes awarded, to overtime, to holidays, to individual permits (whether it is used or not), information relating to absences from work, transferrals to other workplaces, disciplinary measures or proceedings involving the employee.

The above are considered personal data under the guidelines, when they are:

a. contained in acts and documents delivered by the employees during the hiring process (please note that the *Garante* in the past enacted several specific acts regulating the processing of personal data within pre-employment background screening procedures);

b. contained in documents and/or *files* accessed by (or on behalf of) the employer during the work relationship, for the purposes of executing the work contract, and successively gathering, and storing in personal files, papers or on the company's databases;

c. made available in the company's registers, notice boards or *intranets*.

§ 2. The data controller and the data processor of the employees' personal data.

Having considered the general *privacy* principles applicable to the processing of employees' personal data, personal data undergoing processing must be processed lawfully and fairly. In order to ensure compliance, the data must be:

- collected and recorded for specific, explicit and legitimate purposes and used in further processing operations in a way that is not inconsistent with said purposes;
- accurate and, when necessary, kept up to date;
- relevant, complete and not excessive in relation to the purposes for which they are collected or subsequently processed;
- kept in a form which permits identification of the data subject for no longer than is necessary for the purposes for which the data is collected or subsequently processed.

The guidelines clarify the rules aimed at identifying the various different persons who are allowed to process personal data. In particular, the guidelines provide the criteria to identify the "data controller" and the "data processor". With regard to the "data controller" (which the Italian Code on privacy defines as "*any natural or legal person, public administration, body, association or other entity that is competent, also jointly with another data controller, to determine purposes and methods of the processing of personal data and the relevant means, including security matters*") what is important is the effective source/centre of the working relationship, regardless of the company structure adopted. For example, when the personal data are processed within groups of companies, each of the companies has to be

considered as "data controller" with regard to the processing of personal data referring to their employees. Nevertheless, within groups of companies, the subsidiaries or controlled companies may delegate some of the privacy requirements, with the consequence that holding such data will make the organisation to whom it is delegated, the "data processor" of the employees' personal information, which has been provided by the subsidiaries or parent company. It must be pointed out that according to the Italian Code on privacy, the "data processor" is "*any natural or legal person, public administration, body, association or other agency that processes personal data on the controller's behalf*".

Further:

a. the data processor may be designated by the data controller on an optional basis;
b. where designated, the data processor shall be selected from employees who can appropriately ensure, on account of their experience, capabilities and reliability, thorough compliance with the provisions in force applying to processing as also related to security matters;
c. if necessary, on account of organisational requirements, several entities may be designated as data processors also by sub-dividing the relevant tasks;
d. the tasks committed to the data processor shall be detailed in writing by the data controller;
e. the data processor shall abide by the instructions given by the data controller in carrying out the processing. The data controller shall supervise over thorough compliance with both said instructions, also by means of regular controls.

§ 3. Specific aspects of data processing within the Italian decree concerning the improvement of occupational safety and health in all workplaces.

The Italian legislative decree of September 19, 1994 no. 626 (implementing a set of E.U. directives on safety and hygiene in the workplace) specifically provides for the processing of the employees' health data. In particular, this sets out that specific 'sanitary surveillance' on the employees must be carried out. Article 16 of the Legislative Decree 626/94, states that 'sanitary surveillance' includes; preventive controls (clinical, biological examinations and instrumental surveys) carried out in order to ascertain the health conditions of workers, with respect to the risks they may incur. The task of undertaking sanitary surveillance, according to the current provisions, should be assigned to a medicine graduate specialised in preventive medicine of workers and in industrial psychology, industrial toxicology or an equivalent specialisation.

Article 17 of the same legislative decree vests physicians with certain specific functions:

a. carrying out an updated risk health record for every worker submitted to sanitary surveillance, which is to be stored by the employer, with the obligation of professional secrecy;
b. carrying out medical examinations requested by the worker (besides those laid down by article 16) in case such request is linked to professional risks;
c. co-operating with the employer and with the prevention & protection services, to develop, and carry out measures to protect the psychological and physical health of employees;
d. co-operating with the training and information activities of the workers;
e. visiting the workplace at least twice a year and participating in planning the controls of the workers contact with particular agents, whose results must be communicated timely in order to take the proper measures;
f. co-operating with the worker to set up a first-aid service;
g. informing the workers about the sanitary controls they underwent, and in case of contact with agents having long-term effects, about the need to carry out controls even when they stop doing the work which entailed the contact with such agents;
h. informing those employees of the results, for those who want to know about their sanitary controls, and upon request giving them a copy of the relevant documents;
i. communicating with the representatives in charge of the safety, the anonymous collective results of the clinical and instrumental controls which were carried out, as well as explaining their meaning.

In light of the above, the guidelines clarify that the "privacy role" of the physicians is that of an autonomous "data controller" of the employees' personal information, processed according to the mandatory tasks provided by the legislative decree 626/1994.

§ 4. Biometric data and access to "restricted areas"

The processing of employees biometric data, has become increasingly common. *i.e.*, personal information relating to physical features – like the data subject's fingerprints – of individuals that are to be identified uniquely by means of a reference template. The latter consists in a set of digital values that are derived mathematically from the individual features referred to above and are intended to allow identification of an individual via the comparison between the numerical code derived at each access and the initial template.

Fingerprints

Fingerprints are personal data insofar as they can be related to individual employees. Regardless of the fact that only part of them are collected and that they are only used to complete the enrolment phase – as well as the numerical codes subsequently used for comparison purposes. Hence, the provisions laid down in the Italian Code on privacy apply both to the enrolment phase and to any comparison/matching carried out thereafter, including the creation of files relating to an employees' achievements.

The guidelines specify that general and uncontrolled processing of employees' biometric data (especially in relation to fingerprints) is not lawful. Using such data in the workplace may be justified in specific cases, in relation to the purposes and context of their processing – *e.g.*, in connection with accessing certain premises in a company that require especially stringent security measures, either because of specific circumstances, or on account of the activities performed in those areas. Alternatively, their use may be justified in order to ensure security for the processing of the personal data.

In addition to this, the processing at issue could also be regarded as disproportionate, in the light of the envisaged technical arrangements – *i.e.*, the centralised storage of the identification codes derived from the analysis of biometric data. From this

perspective, less invasive technological approaches can undoubtedly be implemented. Bearing in mind the principles set out in Section 3 of the Data Protection Code ("*Information systems and software shall be configured to minimise the use of personal data and identification data. In such a way as to rule out their processing if the purposes sought in the individual cases can be achieved either by using data anonymously, or suitable arrangements to allow identifying data subjects only in cases of necessity*".) One could argue that – providing the use of biometric information is permitted – it is preferable to store the identification code on a medium that is in the data subjects exclusive possession (*i.e.*, a smart card or similar devices) after completing the enrolment phase, rather than recording the codes at centralised level in the companys information system. The latter approach may actually be more prejudicial to individual rights, if the security measures are breached, unauthorised entities access the data, or the stored information is misused – Whether or not by third parties.

Furthermore, the guidelines incorporate the following rules on the processing of employees' biometric data:

a. the data necessary to set up the reference template can be processed exclusively during the enrollment phase; the processing must be based on prior and express consent given by the data subject;

b. in addition to the minimum security measures provided by the Italian Code on privacy, additional measures and guarantees for the data must be adopted;

c. the individuals in charge of the processing must be instructed by means of specific and written guidelines;

d. biometric data – where the processing is allowed – can be stored for a maximum period of 7 days, unless exceptional needs are proved. After such a term has elapsed the data must be erased (even by means of automatic erasure);

e. a preliminary verification on an employers system using biometric data (for example systems or devices for the company security or for the employees' access monitoring by electronic badge) must be requested from the *Garante* if such systems or devices do not comply with the above rules.

§ 5. Communication and dissemination of employee personal data.

The guidelines point out important rules on the communication and dissemination of employee personal data. It is worth mentioning that according to the Italian Code on privacy:

a. *"communication"* shall mean disclosing personal data to one or more entities other than the data subject, the data controller's representative in the State's territory, the data processor and persons in charge of the processing in any form whatsoever (this includes by making available or interrogating such data).

b. *"dissemination"* shall mean disclosing personal data to unidentified entities, in any form whatsoever, including by making available or interrogating such data.

In general, disclosing an employees' personal data to third parties (like employers' associations, trade-unions, parents and relatives, and so on) is allowed where this is based on the data subject's prior consent. Nevertheless, the employer may by-pass the mandatory requirement of consent under the following circumstances, if the processing:

a. is necessary to comply with an obligation imposed by a law, regulations or Community legislation;

b. is necessary for the performance of obligations resulting from a contract to which the data subject is a party, or else in order to comply with specific requests made by the data subject prior to entering into a contract;

c. concerns data taken from public registers, lists, documents or records that are publicly available, without prejudice to the limitations set down by law, regulations and community legislation with regard to their disclosure and publicity;

d. concerns data relating to economic activities that are processed in compliance with the legislation in force as applying to business and industrial secrecy;

e. is necessary to safeguard the life or bodily integrity of a third party;

f. is necessary for carrying out the investigations by a defence counsel referred to in Act no. 397 of 07.12.2000, or else to establish or defend a legal claim, provided that the data are processed exclusively for said purposes, and for no longer than is necessary. Thereby complying with the legislation in force concerning business and industrial secrecy, and with the dissemination of the data being ruled out;

g. is necessary to pursue the legitimate interests of either the data controller or a third party recipient in the cases specified by the *Garante,* and on the basis of the principles set out under the law. This shall also apply with regard to the activities of banking groups and subsidiaries, or related companies. Unless said interest is overridden by: the data subject's rights and fundamental freedoms, dignity or legitimate interests, or if the dissemination of the data is ruled out;

h. Where external communication and dissemination, is carried out by not-for-profit associations, bodies or organisations (whether recognised or not), with regard either to entities having regular contacts with them or to members in order to achieve specific, lawful purposes as set out in the relevant memorandums, articles of association or collective agreements, whereby the mechanisms of utilisation are laid down expressly in a resolution that is notified to data subjects with the information notice;

i. it is necessary for exclusively scientific and statistical purposes in compliance with the respective codes of professional practice, or else exclusively for historical purposes in connection with private archives that have been declared to be of considerable historical interest.

Save for the above, employers are also free to communicate data to third parties when such information are processed anonymously or in aggregate ways (for example: comprehensive number of overtime hours worked, comprehensive economic prizes assigned, etc).

Company's Intranet.

The prior consent of employees is mandatory when the employer wants to make public within the company his/her information (for example: picture, general data, CV's) by means of the intranet (obviously the same consent is required for the publication on the Internet).

Dissemination of employees' data.

Where employers are not allowed to disseminate their employees' personal data through lack of the requirements listed above (a) to (i) or the prior consent, such dissemination is legitimate only when it is necessary for the performance of obligations resulting from the work contract (for example: publication in the company's notice boards of service orders, work shifts, holidays periods, other internal provisions related to the organisation of the work). In other cases, the dissemination of the employees' personal data (even by means of company's notice boards or by means of other internal communications addressed to all the employees) is disproportionate and unlawful, especially when such dissemination is not linked to the execution of work duties. For example, the dissemination is illicit in relation to the following cases:

a. dissemination/publication of salaries, wages or other emoluments referring to personal conditions of the employee;
b. sanctions applied to the employee within disciplinary proceedings;
c. information relating to legal actions regarding the employee;
d. absence from work due to illness;
e. employee membership of associations.

Cards/labels identifying the employees.

The guidelines provide a set of rules about the employees' personal data displayed on identifying cards or labels pinned on their clothing and on work uniforms. Such cards or labels usually aim to improve the relationships between operators and the public. In this regard, the guidelines point out that the obligation to exhibit identifying labels or cards may be founded on the work contract. Nevertheless, with regard to the relationships with the public, it may be disproportionate displaying detailed personal particulars such as; name, surname, date/ place of birth, and photo's on such cards. It is sufficient – in light of their requirement to assist the public, to only display certain information on the ID cards, such as: identifying codes, the sole name of the employee (without indication of the surname), the individual's role, etc…

Methods for communicating personal data.

Save for what is specifically provided by the law, employers must adopt individual forms of communication with the employees, avoiding unlawful communication of personal data (especially when sensitive) to third parties (including to the individuals in charge of the processing within the company), and to anyone other than the interested employee. The guidelines consider the following to be correct forms of communication:

a. addressing communications in closed envelopes;
b. inviting the interested employees to directly collect the communication from the relevant office;
c. sending individual electronic communications to the relevant employee.

§ 6. Processing employees' health data. The security measures.

Specific guarantees must be adopted by the employers in relation to the processing of health data (for example: medical information justifying the employee's absence from work). To this regard, the first mandatory rule is the following:

When the employee delivers to the competent office the medical certification to justify the absence from work, such certificate cannot include the specific diagnosis and may display only the prognosis. Should the employee deliver a medical certification including also the diagnosis, the employer shall have to delete from it the related information.

The second rule is the general prohibition of disseminating the employees' health data.

According to: the Code on privacy, to the collective agreements and to the sectorial laws regulating the labour relationships, employers are allowed to process the following:

a. data relating to employees' illnesses (including information on specialised medical examinations or on clinical checks) when related to the temporary or permanent inability of an employee to work and when necessary for the employers to verify the declared illness;
b. data relating to disabled employees for the fulfilment of legal duties in relation to the so called *"protected categories";*
c. data and documents relating to accidents at work or to illnesses, to be communicated to the public insurance body;
d. health data in general (including the employees' family data) when necessary to allow the employee to apply for particular benefits provided by the law (for example: permits, extended leaves, etc);
e. data relating to drug addiction, when an employee asks to be admitted to particular therapeutic or recovery programs provided by the law;
f. health data to be communicated by the employer to the competent public social security and insurance bodies.

With regard to the mandatory security measures in the processing of the employees' health data, employers must undertake to do the following:

a. ensure that data disclosing health and sex life are processed (both electronically or not) separately from the other personal data allowing employees to be identified directly. *E.g.*, a specific and not generally accessible envelope containing said data must be contained in an employees personal file;
b. adopt measures to avoid abusive access to the employees' data, including the implementation of proper measures aimed at preventing illicit intrusions in the work premises or the illicit gathering of data by other employees;
c. organise training activities for persons in charge of the processing with a view to informing them: of the risks applying to the data, the measures that are available to prevent harmful events, the most important features of personal data protection legislation in connection with the relevant activities, the potential issue of liability and the arrangements to get updated information on the minimum security measures adopted by the data controller;
d. adopt measures in order to ensure data integrity and availability as well as protection of areas and premises, insofar as they are relevant for the purpose of keeping and accessing such data.

§ 7. Privacy rights of the employees.

The first guideline states that employers must provide proper information to employees before commencing the processing of their data. Art. 13 of the Italian Code on privacy provides:

- That the data subject as well as any entity from whom personal data are collected, shall be informed, either verbally or in writing, and even in the cases where the data subject's consent is not mandatory, the purposes and methods used in the processing for which the data are intended.
- The obligatory or voluntary nature of providing the requested data; the consequences if (s)he fails to reply.
- The entities or categories of entity to whom, or which the data may be communicated, or who/which may get to access the data in their capacity as data processors, or persons in charge of the processing, and the scope of dissemination of said data; the privacy rights.

Secondly, employees may exercise the following rights:

a. right of access to the data and to obtain confirmation as to whether or not personal data concerning them exist, regardless of whether such data has been recorded in an intelligible form
b. the right to obtain update, rectifiy or, where interested therein, integration of the data;
c. the right to obtain erasure, anonymisation or blocking of data that have been processed unlawfully. Including data for which retention is unnecessary for the purposes for which they have been collected or subsequently processed;
d. the right to object, in whole or in part, on legitimate grounds, to the processing of personal data concerning him/her, even though they are relevant to the purpose of the collection.

a.right of access to the data and to obtain confirmation as to whether or not personal data concerning them exist, regardless of whether such data has been recorded in an intelligible form

The response provided by employers to the data subject shall include all the personal data concerning him/her that have been processed. Unless the request concerns either a specific processing operation – or specific personal data – or categories of personal data.

Employees' exercise of the above rights may be also permitted with regard to data of non-objective character on condition that it does not concern rectification of, or additions to, personal evaluation data in connection with judgments, opinions and other types of subjective assessment, or the specification of policies to be implemented, or decision-making activities by the data controller.

With a view to effectively exercising the employees' rights, employers shall take suitable measures in order to;

- facilitate access to personal data by the data subjects, even by means of ad hoc software allowing accurate retrieval of the data relating to the individual identified or identifiable data subjects;
- simplify the arrangements and reduce the delay for the responses, also with regard to public relations departments or offices.

Employers must provide employees with complete answers, without limiting the response to the sole list of the categories of information hold. Employers must answer within 15 days from the receipt of the employees request (the term is 30 days in cases of particular difficulty in collecting the requested data).

The data may also be communicated to the requesting party verbally, or else displayed by electronic means – on condition that the data are easily intelligible in such cases (in the light of the nature and amount of the information). The data shall be reproduced on paper or magnetic media, or else transmitted via electronic networks, whenever this is requested.

It must be specified that the employees' right of access regards the data as a such and not the documents. Accordingly, an employee cannot request the delivery of documents, or categories of acts held by the employer. Nor can it be used for the creation of documents not stored in the company's databases or for different aggregation of existing documents. In any case, if the data retrieval is especially difficult, the response to the employee request may also consist of producing or delivering copies of records and documents, which contain the personal data in question.

News

Inquiry reports can include confidential records

By Dr Chris Pounder of Pinsent Masons Solicitors, London. The author may be contacted at chris.pounder@pinsentmasons.com

Reference: Stone v South East Coast. Strategic HA & Others, Neutral Citation Number: [2006] EWHC 1668

The High Court has determined that medical records (and by implication other items of sensitive personal data) which are essential to the findings of an independent inquiry can be published without breaching the Data Protection Act.

The case involved Michael Stone, the notorious murderer of Lin and Megan Russell and assailant of Josie Russell. Following his conviction, Stone cooperated with an independent inquiry into his care, treatment and supervision in the years prior to 1996 and consented to providing his medical history. However, he objected to the publication of its report which was to contain extensive citations from his private medical and psychiatric notes. He argued that in the absence of consent, its publication would constitute a disclosure of medical personal data to the public and that this disclosure would breach the Data Protection Act.

Part of the data protection argument in court rested on the Act's definition of "medical purposes"; this includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services". The court determined that the processing needed to publish the report fell within the ambit of medical purposes as the report itself related to "the management of healthcare services".

The Court noted that other Schedule 3 conditions could apply (e.g. paragraph 7) and that the disclosure was also necessary for the proper functioning of public authorities involved in the inquiry. The judge justified this saying Publication of the report in full can, in my view, only assist the legitimate and ongoing public debate with regard to treatment of the mentally ill and of those with disturbed personalities in the community: which has already resulted, among other things, in extensive proposed revisions to the Mental Health legislation. The judge also noted that Stone had previously consented to his personal data being processed

for the purposes of the report and was also aware that the findings could be made public.

In the public domain

In human rights terms, the judge found that the broad subject matter of the report was already in the public domain including previous publications referring to the detail of his medical and social background. It therefore could not be claimed that such medical information was "private". The judgment also focussed on the strong public interest in accessing information detailing the alleged failings of public authorities, more so where the subject matter relates to public safety and security; these are conditions which can be used to legitimise interference in terms of Article 8. Finally, the judgment concluded that the strength of Article 8 rights must be considered in the context of the Article 10 rights which provided public access to information which the authority wanted to be published.

The Court thus held that the report should be published in full, and that publication would not breach privacy or data protection laws. Stone was given time to appeal, but did not pursue this after the Legal Service Commission refused to provide further funding.

Stop Press: Express Obligations of Confidentiality Affect Privacy Rights

Ian De Freitas, who is a Partner at Berwin Leighton Paisner LLP. Ian can be contacted on Ian.DeFreitas@blplaw.com

The English Court of Appeal has given an important ruling on privacy. As a result it will now be more difficult for the media to justify publishing private information passed to them from someone who owes an express obligation of confidence to the person concerned. What makes the case all the more interesting is that it involves a member of the British Royal family.

The Prince of Wales maintains diaries recording his thoughts on the foreign official visits that he undertakes. One such diary related to his visit to Hong Kong during the handover of sovereignty from Britain to China in the Summer of 1993. A former employee in Prince Charles' private office copied some of the diaries (including the Hong Kong diary) and provided them to a newspaper, The Mail on Sunday. The newspaper published extracts from the diary. The Prince sued the newspaper for breach of confidence and copyright infringement. The finding on the copyright claim is relatively unimportant. The real significance of the decision relates to what the Court of Appeal said about the law of confidence.

At first instance, the Judge gave summary judgement (without a full trial) to the Prince. The newspaper appealed. The Court of Appeal upheld the Judge's decision, but did so primarily on the basis of reasoning that was different from that employed by the Judge.

The Judge approached the case based upon the developing UK law protecting private information. This case law has progressed through landmark decisions such as in the Naomi Campbell litigation. Essentially, following the implementation of the 1998 Human Rights Act, the English courts have carried out a balancing exercise. They have weighed the importance of the right to respect for private life (the Article 8 right) with the right to freedom of expression for the media and others (the Article 10 right). The way that this has been done is to adapt the existing English action for breach of confidence, focussing it less on whether a relationship of confidence (contractual or otherwise) exists between the two parties which has been breached, to instead assessing whether there has been a misuse of private information. This is how the Judge reached his decision, finding in favour of the Prince of Wales.

The Court of Appeal agreed with the Judge's finding for the Prince, but said that the decision should really have rested on a more fundamental point. The former employee of the Prince who had handed a copy of the Hong Kong diary to The Mail on Sunday had entered into an express obligation of confidence with the Prince, that any information in relation to him that was acquired during the course of her employment was not be disclosed to any unauthorised person. The Court of Appeal said that there is an important public interest in upholding express duties of confidence owed by one person to another. Even if disclosure of information is in the public interest, the Court of Appeal said it also has to weigh up whether it is in the public interest to allow the breach of confidence to occur. The Court of Appeal said that when adding this factor to the Judge's reasoning, the Prince's claim against The Mail on Sunday becomes unanswerable.

In summary, when looking at a case involving an express obligation of confidence it is likely to be very difficult to justify publication in breach of that obligation unless the public interest in allowing it is overwhelming.

Another issue that the English courts are currently grappling with is whether the developing law of private information confers rights that can be transferred and enforced by a third party. This is the context of the appeal to the House of Lords in the Douglas -v- Hello litigation. This case involved the film stars Michael Douglas and Catherine Zeta-Jones. It determined that they had the right to exploit their image through an exclusive arrangement with OK Magazine to cover their wedding, such that when covertly taken images subsequently appeared in the rival Hello Magazine, they could successfully sue Hello Magazine for breach of confidence in that respect. Douglas and Zeta-Jones received only modest damages for this invasion of their rights. However, the Court of Appeal denied very much larger damages to the publisher of OK magazine. The court decided that the fact that OK Magazine had a licence from Douglas and Zeta-Jones to use the photographs did not confer on OK Magazine any right of action against Hello Magazine. This point is now before the House of Lords by way of a further appeal. Judgement is expected some time after Easter. The decision is of wider importance because if the House of Lords overturns this decision it is likely to affect whether one media organisation can "scoop" another for a story. Watch this space.

The impact of McKennitt v Ash[1] – English court extends the protection of privacy and confidential information

By Jean-Michel Jost who is a Swiss qualified lawyer in the London offices of Bird & Bird. The author may be contacted on (+44) 20 74156000 or at jmjost@twobirds.com

1. Introduction

The Parliamentary Assembly of the Council of Europe adopted, on 26 June 1998, Resolution 1165 on the right to privacy, which calls upon the governments of the member states to bring into their national law, *inter-alia*, a provision, "which should be made

for anyone who knows that information or images relating to his or her private life are about to be disseminated to initiate emergency judicial proceedings, such as summary applications for an interim order or an injunction postponing the dissemination of the information, subject to an assessment by the court as to the merits of the claim of an invasion of privacy".[2]

1.1 Intrusion Into Privacy and its Remedial Actions

The targets of intrusions into privacy are basically public figures, since details of their private lives serve as an incentive to sales. At the same time, public figures have to recognise that their exposure in society automatically entails increased pressure on their privacy, which to some extent they have no option but to tolerate.

Across Europe, the tendency to extend the protection of private life as set out in Article 8 of the European Convention on Human Rights ("ECHR") can be seen in the leading decision of the European Court of Human Rights ("ECtHR"), *von Hannover v Germany*[3]. But in English law – unlike that of other European jurisdictions including Germany, Switzerland and Italy[4] – there is no general right to privacy expressly stated. These rights have therefore historically only been protected when the facts of a particular case have constituted a recognised pre-existing cause of action such as trespass to property, trespass to the person, harassment, nuisance, defamation, breach of confidence and the like. Consequently, the courts had difficulties to apply the content of article 8 ECHR as such directly to a domestic case. That is also the reason why the proceedings of the *McKennitt* case were based upon alleged breaches of privacy *or* duty of confidentiality. The case finally blazes the trail regarding prospective intrusions into a person's private life by their own associates. Potentially, the decision strengthens and extends the right of privacy.

The general difficulty is that though fundamental, this qualified human right may conflict with a variety of other rights when they are asserted on the same issue, as in the case in question with the ECHR-granted freedom of speech (article 10 ECHR). Since neither article 8 nor article 10 as such has precedence over the other, there frequently arise difficulties in the so-called balancing exercise.

Since the ECHR is now part of English law, incorporated in the United Kingdom's new human rights legislation, the Human Rights Act 1998, the decision has to be in line with the jurisdiction of the ECtHR. In some questions, where no analogy to a precedent judgment of the ECtHR can be drawn, it is the judge's task to advance the argumentation in the sense of the ECtHR. This decision, in so doing, clearly affirms a shift in favour of the protection of private life and confidential information in accordance with the ECtHR decision in *von Hannover v Germany* stating that even a legitimate interest in a public figure cannot of itself justify an intrusion into their private life, even though over the past years the English courts have angled off from denying the right of privacy per se as a cause of action.

Recent English cases such as *Campbell v Mirror Group*[5], although decided before the *von Hannover* decision was published, have highlighted that even persons who are in the public focus should still reasonably and legally be entitled to have a level of protection of their privacy, just like ordinary people of no significance in contemporary society. The balance of interest has to be performed equitably in both cases, considering the same elements of assessment. The outcome of the degree of protection of their private life cannot be equivalent, however, because public figures step willingly onto, or at least accept their appearance on, the public stage and therefore cannot expect the same protection as the latter. By virtue of their degree of celebrity and their conduct on the public stage, their claim for protection of their privacy is automatically restrained compared to unknown people living their life unperceived by the public.

1.2 Summary of Facts

Loreena McKennitt is a famous folk musician of Canadian origin with an international reputation. Aside from her primary livelihood, she also owned two related companies. She gave a number of live concerts worldwide and sold millions of albums.

Niema Ash and her long term companion, Tim Fowkes, were her closest friends. Both worked for a limited period for Ms McKennitt within her profession and even accompanied her on a tour abroad. Thereafter Ms Ash agreed to assume the promotion of the newly released album "The Book of Secrets" on the occasion of a tour in Europe and America, as a merchandising supervisor.

After a quarrel, however, the relationship between Ms McKennitt and Ms Ash and her companion broke apart. This swayed Ms Ash to publish in 2005 a book entitled "Travels with Loreena McKennitt: My life as a friend" revealing, *inter alia*, personal and confidential issues about her former friend. Ms McKennitt claimed the book breaches her privacy and a duty of confidence, which arose in some instances by contract or otherwise was implied by law. Certain statements in the book were alleged to be false.

At first instance, Eady J granted Ms McKennitt an injunction prohibiting the publication and sale of Ms Ash's book. The Court of Appeal has now upheld that decision.

1.3 General Remarks

This most recent English decision of the Court of Appeal in this field is significant because despite the increase in litigation in this field over the last decade, there remain several previously unexplored issues relating to the right of privacy.

The significance of this case is also shown by the fact, that the Premier League of the British media industry[6] sought permission as a non-party to intervene. For these stakeholders it is essential to know where the balance has to be struck between the right to privacy and freedom of expression. The answers to these legitimate questions delineate how far the media can go in pursuing information about public figures such as Royalty, politicians, academics, actors, or in this case, singers.

2. Scope of the Right to Respect for Private Life (Art. 8 ECHR)

The scope of a right to personal privacy is difficult to define, because it consists of a bundle of rights which have a variety of justifications[7]. The specific right to respect for private life under article 8 ECHR protects both personal identity[8] and individual self-determination as well as the free organisation of one's own lifestyle. Article 8 ECHR protects not a general freedom of action, but nevertheless substantial ranges of the personal lifestyle and the individual's physical and psychological integrity, particularly with regard to the social context. The right may include activities of a professional or business nature. There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life".[9] Article 8 applies therefore not only categorically to the most personal and intimate sphere, but also to private behaviour which takes place before the public. The range and extent of the protection depend on the

public figure's degree of celebrity and their behaviour on the public stage.

3. Balancing Exercise Between the Right to Respect for Private Life (Art. 8 ECHR) and Freedom of Speech (Art. 10 ECHR)

The protection of private life has to be balanced against the freedom of expression guaranteed by Article 10 of the Convention. In that context the *McKennitt* judgment emphasises "that the freedom of expression constitutes one of the essential foundations of a democratic society. Subject to paragraph 2 of Article 10, it is applicable not only to "information" or "ideas" that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb. Such are the demands of that pluralism, tolerance and broadmindedness without which there is no democratic society".

One should also consider the substance of the information transmitted to the public: whether the revelations have mainly an entertaining or an informative character. The ratio of article 10 ECHR, as the Court understands its content, is to stimulate the public debate essential for a democratic society. In *von Hannover v Germany* the ECtHR contemplates "that a fundamental distinction needs to be made between reporting facts – even controversial ones – capable of contributing to a debate in a democratic society, relating to politicians in the exercise of their functions, for instance, and reporting details of the private life of an individual who … does not exercise official functions. While in the former case (*Observer and Guardian*) the press exercises its vital role of "watchdog" in a democracy by contributing to "imparting information and ideas on matters of public interest", it does not do so in the latter case".[10]

It is necessary to consider the media's freedom of expression and the corresponding interest of the public in being informed on the one hand, and, on the other hand, the legitimate expectation of each individual to have their private life protected. *McKennitt* establishes that a person cannot publicly reveal their own private life and thereby expose confidential issues regarding which others are entitled to protection, if the others' consent is not forthcoming. Even in cases where there is a real public interest in the information paired with a potential commercial interest in publication by both discloser and the media, these interests have to yield if the individual's right to respect for private life outweighs them.

The exercise requires an intense scrutiny of the specific facts to determine whether the particular information merits protection. In *McKennitt* Mr Justice Eady stated: "it is thus necessary to scrutinise with care any claim to public interest – which are sometimes made by the media and their representatives on a rather formulaic basis". In this case, the information Ms Ash proposed to reveal to the public included personal and sexual relationships, Ms McKennitt's mental condition relating to the drowning of her fiancé, her health and diet as well as emotional vulnerability. These were in the judge's view exclusively details of her private life and would not contribute to a debate of general interest.

4. Information Entrusted to Third Parties

An obligation of confidence may have its origin in contract, tort, equity or bailment or be imposed by statute. Whatever its origin, it is of high significance in governmental, commercial and personal contexts. To be confidential, information must possess two indispensable characteristics:

a. limited public availability; and

b. specific character, capable of clear definition. If either basic requirement is missing, the information cannot be qualified as confidential, hence cannot be protected even though it is expressly declared as confidential. (Nevertheless, a notation of information as confidential could in marginal cases, be crucial.)

The duty of confidence protects the *substance* of the information, in contrast to copyright which protects merely its form of expression. For instance, the obligation of confidence protects an invention prior to the grant of a patent or may represent an alternative way of protection to patenting, if the invention is not disclosed to the public through sale of a product. Furthermore, present and former employees can be bound by an obligation of confidence to protect trade secrets and goodwill against abuse.

The difficulty arises in ascertaining where a mutual trust, respective of an obligation of confidentiality, accrues outside the contractual context. Particularly in private contexts, one is confronted with duties of confidence of such origins. The issue is whether the necessary level of confidence is – if at all – reached to induce an obligation of confidence. The media are increasingly frustrated by judges who are progressively more willing to find an obligation of confidence, which can also bind third parties, such as the media, who obtain or acquire information and are in a position where they can or ought to know that this information is confidential.

5. The Legal Status of Confidential Information

After having established the existence of confidential information, it would be very useful to know the exact legal status of confidential information in order to proceed to the next step of assessment as to whether the revelation of that information to the public is illicit. Unfortunately, there is no contemporary English decision on this question. The editors of *Halsbury's Laws of England*, the leading compendium of English laws, offer some interesting reflections about the legal qualification of confidential information:

"An entrustment of confidential and intangible material may, however, be treated as a bailment of information, creating rights and duties akin to those which arise under a true bailment; this is on the basis that *confidential information can be property*. There is no direct authority that information may be the subject of a bailment, but there are decisions which appear to favour an analogy between bailment and the entrustment of information, or which use the language of bailment in describing such entrustment. If the analogy is accepted, a person to whom confidential information is entrusted can be restrained, by means of remedies akin to those arising on a bailment, from dealing with the information contrary to the terms of the entrustment, and monetary remedies can be awarded in similar fashion to those which issue in respect of interference with chattels".[11]

It is clear that in such a proceeding it would be difficult to substantiate the value in capital of confidential information, but it would further strengthen the basis for a privacy action and

the addressees of such information would become probably more conscious about its significance.

In *McKennitt v Ash*, Eady J appeared to accept that confidential information is qualified as property:

"If information is my private property, it is for me to decide how much of it should be published".

The Court of Appeal in *Douglas v Hello!*[12] on the other hand concluded firmly that information cannot be treated as a property right; this point is under appeal to the House of Lords in that case. Of course, should the property argument be accepted there may emerge a legitimate concern about the possibility of censorship by public figures, in that they could control absolutely all information about themselves. To balance this risk, the legal argument of "public interest" in disclosure must intervene. But at this point one has to ask if there exists a legitimate public interest in receiving this information.

6 Freedom of Expression

Ms Ash was given permission to appeal Eady J's decision only on the grounds of her potential right of article 10 ECHR "freedom of expression". A duty of confidence arises purely from the fact of her very close relationship to Ms McKennitt. Ms Ash was allowed to take part in McKennitt's private life precisely because of her manifested confidence vis-à-vis her. Information deriving from McKennitt's private life was therefore confidential in Ms Ash's hands. Nevertheless, by means of the construct of "shared experience", the appellant tried to justify her revelation to the public of the information she had acquired.

The nub of this argument is whether the revealed story originates objectively from the same person's privacy or whether another's privacy is affected. On the facts of the case on hand, it was clear that Ms Ash "had no story to tell that was her own". She revealed rather Ms McKennitt's private life, to attract a readership who know Ms McKennitt as a folk singer and wish to know more about her.

Because of the appellant's relationship with McKennitt, she either knew or ought to have known that Ms McKennitt could reasonably expect her privacy to be protected. *A fortiori* this is so when she was plainly aware of the importance Ms McKennitt attached to keeping her private life shielded from public eyes. This consciousness was also expressed by Ms Ash in her book: "She cared for us and we cared for her. We were her closest friends and she knew she could count on our unqualified loyalty". Ms Ash was also aware that Ms McKennitt protected her reputation and privacy "with the iron safeguard of a chastity belt". These passages alone were enough to affirm unreservedly the mutual expectation of confidence. As Eady J stated, "the provisions of the written contract did not add much to the obligations that Ms Ash owed in equity by reason of the closeness of her personal relationship with Ms McKennitt".

7. Public Interest and Public Domain

Ms Ash attempted to justify the disclosures made of the above-mentioned issues by relying on the public interest and on the defence that Ms McKennitt had put some of the matters – her feelings relating to her fiancé's death by drowning – into the public domain so that there could no longer be any confidentiality with respect to these. This zonal argument – that once a person had made public some particular information falling within a particular "zone" of his or her life, he or she had a greatly reduced expectation of privacy in relation to any other information that fell within that zone – was rejected. This was on the basis that such an approach would "completely undermine the reasonable expectation of privacy, and the subject's right to decide how much, and what kind of private information about him or her can be published". Disclosed information from a particular area of private life does not mean that an exhaustive revelation of this zone cannot be prevented by the individual concerned.[13] This is a further unsatisfying aspect for the media. It will be interesting to see if this argument will be picked up again in a future case focusing on this problematic.

Of course, it also depends on the extent of the disclosed information and the number of the addressees. The Court of Appeal in *McKennitt v Ash* stated that "the general principle is no doubt correct …, information that is already known cannot claim the protection of private life". The court will not, however, refuse a preliminary injunction because the information has become known to a narrow subgroup of the public or is accessible by persons with some degree of background knowledge. However, there is a threshold where it is plainly meaningless to pretend that there is any confidential information left to be preserved.[14]

8. Infringement of Privacy by False Information

Defamation and false information without a defamatory character, which can nevertheless have a negative impact on the concerned individual, fall obviously in the scope of application of the article 8 ECHR because following the jurisdiction of the ECtHR the psychological integrity of each citizen of the member states shall be protected. The distinction between breach of confidence, which protects the right of privacy, and defamation, which is an act of communication that puts a person in a harmful light can be somewhat troublesome. To obtain relief against a statement on the grounds of defamation, it must be proven false,[15] while to file an action for breach of confidence, the act or information complained of must be true, but have been revealed in breach of confidence.

In *Interbrew SA v Financial Times Limited* [16] Sedley LJ held that "there can be no confidentiality in false information". Nevertheless, in the light of the development of the jurisprudence on privacy since that decision, it is possible that where false information is spread out in the public and its content has not at all a defamatory character, then a privacy claim would be permitted to proceed, although the concerned individual would not be entitled to recover general damages for injury to his or her reputation. In this case the claimant would be entitled only to a grant of a right of rectification.

Even though there is a certain double-think involved in claiming a reasonable expectation of privacy in relation to information which, being false, in fact does not relate to a person at all, it is clear that it can be highly intrusive, for instance, if someone makes false allegations about another

person's state of health or personal relationships. At the very least, such statements pressurise the concerned party to disprove these allegations through revelation of his health situation. The expectation would have to be claimed in relation to any statement as to a zone of life, such as physical or mental health, which would in normal social relations be considered private.

9. Legal Practice

In the last years there have been an increasing number of privacy claims against the media. From prior decisions and the decision in *McKennitt v Ash* the following tests are to be applied:[17]

1. The party bringing the complaint has to prove by evidence a genuine threat to publish the particular material he or she seeks to restrain.
2. The complainant likewise has to show he or she has a *reasonable expectation of privacy* in relation to the material (the threshold test). This criterion can equally be defined by the question: is Article 8 engaged at all?
3. Since the Article 10 right to freedom of expression is invariably engaged – whatever the information concerned may be – the court must then embark on a balancing exercise, weighing the competing rights. What degree of interference would publication do to the Article 8 right compared to the interference an injunction would do to the Article 10 right (test of proportionality)?

Various criteria which are taken into account by the courts for the balancing exercise include:

- Exposure to the public of the person in question: Here we have to analyse the general conduct of the person on the public stage (public eye);
- Does the complainant carry out any official functions?
- Does the revealed information in fact derive from the complainant's private or public life?
- Degree of celebrity of the subject;
- Duration of the intrusive actions;
- The degree of intrusiveness of the conduct by which the information was obtained; and
- The substance of the information proposed to be revealed (entertaining character or genuinely informative?);
- The truth or falsity of the information;
- The existence and nature of any public interest in the disclosure.

10. Conclusion

In recent cases, where a public figure could demonstrate a "reasonable expectation of privacy" the courts have been willing to uphold his or her right to private life over the right to freedom of expression or the right to be informed.

One negative point in the various judgments of the ECtHR is that Court has used different determinative tests to ascertain and assess the balancing exercise. The guidance of "reasonable expectation of privacy" which was set out in *Halford v United Kingdom*,[18] and has been adopted in the leading English cases since then (although not in *von Hannover v Germany*) makes redundant the sometimes very difficult assessment as to whether a person qualifies as a public figure. The "reasonable expectation of privacy" approach requires an assessment on the facts of each individual case.

The balancing exercise between the two particular competing interests, articles 8 and 10 ECHR will remain one of the most difficult tasks for judges to perform. Both rights cannot co-exist in their fullest form, hence a protection of one necessarily narrows the other. Evaluating the individual elements of a special case is inevitably a matter of subjective opinion. One has to keep always in mind that the term "privacy" or "private life" is a moving feast; even in future cases it will be almost impossible to draw an exact borderline between what can be resisted as an intrusion of privacy and what cannot. Nevertheless, in *McKennitt v Ash* the protection of privacy and confidential information appear to have undergone considerable extension; suggesting that the English judges will apply the decisions of the ECtHR in preference to earlier, narrower judgments of the English courts.

1 Niema Ash and another v Loreena McKennitt and others, 2005 EWHC 3003 (QB); 2006 EMLR 178

2 Resolution 1165 (1998) of the Parliamentary Assembly of the Council of Europe on the right to privacy, para. 14 (vii).

3 59320/00 2004 ECHR 294. The decision in this case was striking, where photographs of substantially banal activities in public were held an infringement of the right to private life. Nevertheless, this decision has to be interpreted with caution, because in this case the intrusion was of a long duration.

4 See for instance: Right to protection of personality (Persönlichkeitsrecht), guaranteed by sections 2(1) and 1(1) of the Basic Law (Grundgesetz) and the protection of privacy (Schutz der Privatsphäre), guaranteed by the article 13 of the Swiss Federal Constitution and the protection of privacy by articles 2, 13, 14 of the Italian Constitution.

5 2004 UKHL 22

6 Times Newspapers Ltd, Telegraph Group Ltd, Associated Newspapers Ltd, The Press Association, British Sky Broadcasting Ltd and BBC.

7 see discussion in Halsbury's, Constitutional Law and Human Rights, vol 8(2) (Reissue) para 110.

8 Burghartz v Switzerland, 16213/90 1994 ECHR 2

9 Peck v the United Kingdom, 44647/98 2003 ECHR 44, para 57:" See also Amann v Switzerland, 27798/95 2000 ECHR 88 Niemietz v Germany, 13710/88 1992 ECHR 80 and Halford v United Kingdom, 20605/92 1997 ECHR 32.

10 see von Hannover v Germany op cit, para. 63

11 see Halsbury's, Laws of England, Fourth Edition, 2003 Reissue, vol 8(1), para 408

12 2005 EWCA Civ 595

13 On the other side the zonal argument can also be too broadly construed: If an individual reveals a particular area of his or her private life, he or she can hardly rely on the principle of reasonable expectation of privacy if others wish to disclose information of this individual in similar kind and in similar detail.

14 AG v Guardian Newspapers ("Spycatcher") 1988 3 All ER 545

15 unless the defendant does not raise a defence of justification

16 Interbrew v Financial Times Limited 2002 EMLR 446

17 Checklist taken from Andrew Caldecott, QC's speech "The Law of Confidence & Privacy – overview of leading cases & canvassing the principles governing the grant of interlocutory injunctions" on February 26th 2006 at Bird & Bird, London, UK.

18 Halford v the United Kingdom, 20605/92 1997, ECHR 3222

  WDPR ISSN 1473-3579

Security & Surveillance

The Golden Rule of Privacy: A Proposal for a Global Privacy Policy On Government-to-Government Sharing of Personal Information

Global Privacy – Cross-Border Information Sharing

By John W. Kropf *the Director of International Privacy Policy for the Department of Homeland Security's Privacy Office. The views expressed here are his and not those of the Department of Homeland Security or the U.S. government.*

As the United States prepares to enter into a new arena of cross-border sharing of personally identifiable information, it would be well served to adopt a global strategy. John Kropf, of the Department of Homeland Security's Privacy Office, suggests an approach based on the Fair Information Practices combined with the basic international principle of reciprocity. The end result, Kropf writes, would be improved international co-operation combating terrorism and protection of the privacy of legitimate international travellers.

I. Introduction

The U.S. government is on the cusp of implementing a series of international agreements to share personally identifiable information (PII) with its allies and friends. Systematic cross-border sharing of PII between governments is still a relatively new area in international relations. The United States itself is still formulating a policy framework to allow for the strategy sharing of PII. Despite several legal and policy initiatives that have been in place for two or more years, implementation has been limited. This paper suggests an approach based on the Fair Information Practices (FIP) combined with the basic international principle of reciprocity.

II. The Issue: International Information Sharing Authorities

Since Sept. 11, 2001, the United States has created new authorities and established new ways to work with foreign partners to improve U.S. access to information on international travellers and on individuals involved in terrorist activities. Examples include the Secretary of State's authorisation under the USA PATRIOT Act of 2001 to make agreements with foreign governments to share information from the visa lookout database for the purpose of fighting terrorism;[1] Homeland Security Presidential Directive 6 (HSPD-6)[2] that tasked the Secretary of State to seek ways to access terrorist biographic screening information from foreign partners; and the Regional Movement Alert List (RMAL), a regional initiative within the Asia Pacific Economic Co-operation (APEC) to share lost and stolen passport information.[3] Among the most discussed examples lately, is the exchange of airline passenger information – known as Passenger Name Record (PNR) data – an agreement that the Department of Homeland Security (DHS) entered into with the European Commission (E.C.) to enable the transfer of this information.[4]

The 9/11 Commission recognised the critical role information sharing plays in the fight against terrorism when it recommended that:

The U.S. government cannot meet its own obligations to the American people to prevent the entry of terrorists without a major effort to collaborate with other governments. We should do more to exchange terrorist information with trusted allies, and raise U.S. and global border security standards for travel and border crossing over the medium and long term through extensive international co-operation.[5]

The Commission singled out exchanging lost and stolen passport information as having immediate security benefits that are particularly important so long as it is consistent with privacy requirements.[6]

Meanwhile, implementation of these new authorities has been limited due to the complexity of harmonising different frameworks. As of this writing, an interim agreement on the transfer of PNR data between the European Union and United States and two APEC Lost and Stolen Passports (LASP) MOU's[7] have been completed and put into operation.[8]

III. A Suggested Global Approach

This paper recommends a global privacy strategy based on both substance and structure. Since the mechanism for sharing has been or is expected to be bi-lateral and multi-lateral arrangements in the form of Memoranda of Understanding (MOU) or other international instruments, this strategy is centred around building a model agreement. The starting point for substance of the arrangements should be the "Fair Information Practices" (FIP). These practices can serve as a common frame of reference and template to guide drafting provisions concerning PII.

A. Substance: Fair Information Practices (FIP)

The FIP were first articulated as a result of a 1973 report by the U.S. Department of Health, Education, and Welfare advisory committee that identified eight practices, known as the FIP. The report, which served as the basis for the U.S. Privacy Act of 1974, listed the following practices:

- *Collection limitation principle* – data should be obtained lawfully and fairly;
- *Data quality principle* – data should be relevant to the purposes for which it will be used, accurate, complete and up-to-date;
- *Purpose specification principle* – the purposes for which data will be used should be identified at the time of collection;

- *Use limitation principle* – personal data should not be used for purposes other than those specified except with the consent of the individual or by authority of law;
- *Security safeguards principle* – procedures to guard against loss, corruption, destruction or misuse of data should be established;
- *Openness principle* – it should be possible to acquire information about the collection, storage and use of personal data;
- *Individual participation principle* – the data subject normally has a right of access and to challenge data relating to her; and
- *Accountability principle* – a data controller should be designated and accountable for complying with measures to give effect to the principles.
- The FIP, which are the foundation of the Privacy Act of 1974, also allow for flexibility for national security and law enforcement considerations.

Internationally, the U.S. government has long promoted the FIP. In 1980, the FIP served as the basis for the 1980 *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD Guidelines) issued by the Committee of Ministers of the Organisation for Economic Co-operation and Development (OECD).[9] All 30 member states adopted the OECD Guidelines, including 15 members that are also members of the European Union. As recently as 2004, the FIP principles were championed again by the United States within the 21-member "economies" of APEC. The APEC Privacy Framework was also based largely on FIP principles.[10] The benefit of the OECD and APEC frameworks is that they stress flexibility between systems and ways to reduce barriers to trans-border data flows.

For the United States, FIP have been embedded into its existing bilateral arrangements, such as the U.S. MOUs on LASP with Australia and New Zealand,[11] a model MOU on LASP endorsed by all APEC economies, and, to some extent, in the interim United States – European Union PNR arrangement contrast to the E.U. privacy framework.[12] Therefore, based on this initial success, the FIP can serve as a proven framework for negotiating further international arrangements.

B. Structure: Reciprocity – A Cornerstone of International Agreements

The second element to the global strategy is the principle of reciprocity. Reciprocity is defined as exchanges of roughly equivalent values in which the actions of each party are contingent on the prior actions of the others in such a way that good is returned for good, and bad for bad.[13] Some commentators have declared that reciprocity is a "condition that theoretically attached to every legal norm of international law."[14] Indeed, it is a fundamental structure of many international agreements,[15]including arms control, trade and commerce, and law enforcement. Even the U.S. Supreme Court has observed, "Public officials should bear in mind that 'international law is founded upon mutuality and reciprocity …"[16]

1. Protection of U.S. Persons Around the World

One of the most relevant examples of reciprocity is the granting of privileges, protections or other treatment to nationals of other states. Examples include treatment of diplomatic personnel,[17]consular rights of foreign citizens,[18] and visa requirements.[19] For instance, the protection of American citizens abroad is based on a reciprocal obligation under the Vienna Convention on Consular Relations. In general, consular obligations require that a foreign national be treated as we would want an American citizen treated in a similar situation in a foreign country. As a specific example, where an American is detained by the authorities of a foreign government, that individual must be given prompt access to an American consular official and vice versa.

Similarly, protection of Americans' PII should be no different and should also be treated under the principle of reciprocity. A decision on whether to apply reciprocity to the processing of a foreign citizen's PII will directly affect the United States' ability to protect information on American travellers overseas. Indeed, leadership at DHS, an agency actively involved in cross border information sharing, recently underscored the principle of reciprocity in the field of international data sharing:

If we want to protect the privacy of our own citizens, we are going to have to be willing to protect the privacy of our international partners and their citizens. And that means we have to protect shared information and continue to demonstrate a level of trust ... I trust that the Privacy Office will be equally vigorous in insuring that American data is protected in the European Union to the same or a higher degree.[20]

As with the U.S. system, our allies and friends have their own obligations to ensure the privacy of their citizens' information. Failure to offer U.S. partners such commitments could reduce their incentive to protect U.S. person PII and frustrate the long-term U.S. government counter-terrorism objectives.

2. Greater Likelihood of Advancing Long Term U.S. Interests

As a practical matter, a strategy of reciprocity will also improve the United State's chances of success in achieving PII sharing arrangements. To reiterate, reciprocity is a principle of international agreements that is widely understood and accepted by governments around the world. Further, reciprocal arrangements can work in both bi-lateral and multi-lateral situations.[21]

a. Domestic Recognition of Privacy Interests of non-U.S. Persons

DHS set the foundations for recognising the privacy interests of non-U.S. persons early in its existence. At the beginning of 2004, DHS initiated the US-VISIT program, a major border management system that collected personal information including biometrics. US-VIST made a policy commitment to extend privacy protections to non-U.S. persons.[22] While a literal reading of the Privacy Act of 1974 limits the law's application to U.S. citizens and lawful permanent residents (LPRs),[23] DHS policy makers were mindful of the need to extend privacy protections to non-U.S. persons. They realised that a policy commitment to extend these safeguards would not only build trust in the international travelling public, but it would also advance our strategic goal of cross-border information sharing. DHS intended to rely heavily on access to foreign visitor information; this policy assured foreign governments that their citizens' information would be safeguarded. Such a policy was likely to make U.S. foreign partners more receptive to future co-operation on sharing PII.

b. International Recognition of non-U.S. Persons

Building on the DHS domestic policy commitment to non-U.S. persons, a joint Department of State and DHS team entered into reciprocal commitments to privacy in the case of the LASP MOUs with Australia and New Zealand. Specifically the FIP principles were incorporated and applied on a reciprocal basis. Both MOUs contain the following reciprocal language:

CONDITIONS OF USE

The receiving Party intends to use its best efforts to maintain any personal/biographic or other related information received in accordance with Article IV.C. in the same manner as it maintains information concerning its own citizens, unless the receiving Party is required to do otherwise under its laws. In the event that the same protection is not available, the receiving Party should inform the other of this fact and the reason that the protection is unavailable.[24]

Because the MOUs were policy commitments – and not legal obligations – such a pledge did not create any new legal right for non-U.S. persons under the Privacy Act or other U.S. laws. The MOUs were simply a pledge to use best efforts to apply FIP principles to non-U.S. persons.

In contrast, the 2004 PNR negotiations with the European Union offer an example of how failure to offer privacy protections at the outset can create a challenge in negotiating an agreement. Although the PNR agreement was eventually concluded in May 2004, the perception that the United States did not respect the privacy interests of all persons created significant international challenges for the U.S. government, adding an entire year to completion of the negotiations. Part of this negative perception may have come from the limited protection of the Privacy Act. In an effort to dispel the misperception that the United States offered no privacy protection to non-U.S. persons, significant time and effort was devoted to explaining to our E.U. partners the three-part U.S. privacy framework (Privacy Act, Freedom of Information Act, E-Government Act of 2002).[25]

Ultimately, the E.U.-PNR Undertaking's privacy protections for non-U.S. persons were based upon a combination of existing U.S. law, regulations, Customs and Border Protection (CBP) policies and procedures, and the representations made in the Undertakings. The conclusion of the negotiations for the E.U.-PNR agreement was assisted by the privacy protections the United States was able to offer with respect to treatment of information on non-U.S. persons. In short, this was an international policy commitment to afford non-U.S. persons with similar protections to those afforded U.S. persons under the Privacy Act.[26]

V. Conclusion

As the United States prepares to enter into a new arena of cross-border sharing of PII, it would be well served to adopt a global strategy. A tandem approach based on the substance of the FIP principles and the structure of reciprocity would be well suited to meet this challenge. FIP principles have been implemented domestically and endorsed as a framework internationally. They have also proven to be flexible enough to adapt to allow the United States to meet its security interests while at the same time protecting privacy. Likewise, reciprocity is a principle of international agreements that is widely understood and accepted. Reciprocal obligations to process PII will serve to protect the privacy of Americans' PII as well as assist the United States in implementing the international arrangements necessary for the flow of this information. The end result is improved international co-operation combating terrorism while protecting the privacy of legitimate international travellers.

If we want our partners to ensure protections to PII collected about U.S. persons, a strong commitment to honour privacy protections for non-U.S. persons, as demonstrated through reciprocal application of the FIP principles, will protect Americans around the world and improve our chances for success. In short, we want to be in a position to be able to follow the Golden Rule and say, "we'll give your people the same privacy you gave our people." To do otherwise would put the U.S. government in an untenable position of seeking a double standard.

1 Section 222(f) Immigration and Nationality Act (8 U.S.C. sec. 1202(f)) as amended by section 413 of the USA PATRIOT Act of 2001, Act of Oct. 26, 2001, Pub. L. No. 107-56, 115 Stat. 272.

2 Section 5, HSPD-6, Sept. 16, 2003. The Directive's implementing MOU stipulates that the Parties will make accessible appropriate information to foreign governments cooperating with the United States in the war on terrorists of global reach.

3 APEC News Release at *www.apec.org/apec/news___media/media_releases/270206_vn_rmal.html* RMAL is a specific security commitment that APEC Leaders called for in the Enhancing Human Security section of the 2003 Bangkok Declaration and 2004 Santiago Declaration. See also the Department of State policy initiative to share lost and stolen passport data with foreign governments as articulated by Frank E. Moss, Deputy Assistant Secretary for Passport Services Bureau of Consular Affairs, Address to the International Relations Committee, U.S. House of Representatives (June 23, 2004).

4 The PNR Agreement and Undertakings can be found at *http://europa.eu.int/comm/external_relations/us/intro/pnr.htm*. While the Agreement was determined to be invalid by a May 30, 2006, European Court of Justice decision, its provisions are nevertheless useful to understanding cross border data flows of personal information.

5 The 9/11 Commission Report (New York: W.W. Norton & Company), 390.

6 Id., 389.

7 APEC News Release at *www.apec.org/apec/news___media/media_releases/270206_vn_rmal.html*

8 In September 2006, a model MOU for all APEC members on LASP was ratified.

9 OECD Guidelines can be found at: *www1.oecd.org/publications/e-book/9302011E.PDF.* The Guidelines represent an international consensus of the OECD's 30-member countries, many of whom are also member states of the European Union.

10 The APEC Framework can be found at www.APEC.org.

11 Available at *www.apec.org/apec/documents_reports/informal_experts_group_business_mobility/2006.html.* Both MOUs were non-binding international executive agreements, or political commitments. An international agreement done without advice and consent of the Senate is an ''international agreement other than a treaty'' for purposes of U.S. domestic law; this category of international agreement includes ''executive agreements,'' which are done pursuant to the President's constitutional authorities. This category of international agreements also includes agreements done pursuant to U.S. authorising legislation. For international law purposes, both categories are considered to be ''treaties,'' including as defined by the Vienna Convention on the Law of Treaties (VCLT), insofar as they are international agreements between two or more states or international organisations and are intended to be legally binding and governed by international law. While the United States is not a party to the VCLT, it accepts the VCLT's definition of a treaty as consistent with customary international law. For example, a legally binding instrument contains terms such as ''shall'' or ''will'' as compared to a political

document which contains terms such as ''intends to'' or ''understands.''

12 See PNR Undertakings at note 5, infra.

13 Robert O. Keohane, *Reciprocity in International Relations*, 40 INT'L ORG. 1 (1986), p. 8.

14 Elizabeth Zoller, *Peacetime Unilateral Remedies* (Dobbs Ferry, N.Y.: Transnational, 1984), p. 15.

15 Arthur Nussbaum, *A Concise History of the Law of Nations* (The Macmillion Co., New York, 1954); Keohane, Ibid.

16 *Breard v. Pruett*, 134 F.3d 615, 622 (4th Cir.), cert. denied sub nom. *Breard v. Greene*, 118 S.Ct. 1352 (1998) quoting *Hilton v. Guyot*, 159 U.S. 113, 130 (1895).

17 Vienna Convention on Diplomatic Relations (VCDR), April 18, 1961, 23 UST 3227, 500 UNTS 95.

18 Vienna Convention on Consular Relations (VCCR), Apr. 24, 1963, 21 UST 77, 101, 596 UNTS 261.

19 See for example the statutory provisions of the Visa Waiver Program and the period of validity of visas 8 U.S.C. §§ 1187, 1201(c).

20 Secretary Chertoff's prepared remarks delivered by Mr. Paul Rosenzweig, Counsellor to the Policy Directorate before the DHS Privacy Advisory Committee, Dec. 6, 2005, available online at: *www.dhs.gov/xoig/assets/mgmtrpts/privacy_advcom_12-2005_mins_am.pdf*

21 Keohane *Reciprocity* supra note 13.

22 *www.dhs.gov/xtrvlsec/programs/editorial_0678.shtml*

23 The Privacy Act applies to ''a citizen of the United States or an alien lawfully admitted for permanent residence.'' 552a(a)(2). For ease of reference, this article will refer to those covered by the Privacy Act as "U.S. persons" and those not covered as "non-U.S. persons."

24 See note 11

25 See Privacy Office Annual Report 2004, available online at: *www.dhs.gov/dhspublic/interapp/editorial/editorial_0338.xml*

26 Coincidently, the PNR Agreement incorporates an element of reciprocity but not directly related to PII protections. At the time the Agreement was signed, PNR information was flowing in one direction – from the European Union to the United States. It was anticipated, however, that the European Union would eventually request PNR information from the United States on persons travelling from the United States to the European Union. Indeed, the European Union has already initiated plans to collect PNR data on travellers entering from outside its Member States. The PNR Agreement contemplated this possibility by including a reciprocity clause in paragraph six which ensures the future assistance of the U.S. government, if the European Union or its Member States were to introduce such a system requiring U.S. airlines to transfer PNR data to E.U. authorities.

News

BELGIUM

Privacy Commission Considers Whistle-blowing Hotlines

By Sylvie Rousseau, an Associate in the Brussels office of Linklaters. The author may be contacted at sylvie.rousseau@linklaters.com

November, 2006 – the Belgian Privacy Commission issued a recommendation setting out how a whistle-blowing system could be established in compliance with the Belgian Data Protection Act (the "DPA"). This recommendation follows the opinion of the Article 29 Data Protection Working Party, as well as the opinions of the French and Dutch data protection authorities.

The main principles in the recommendation are as follows:

Legal grounds

A whistle-blowing system will only be justified if:

(a) it is based on a legal obligation imposed on the company under Belgian law. An obligation imposed by a foreign law is not a valid ground; or

(b) it is in the legitimate interest of the company, unless the interests and rights of the person to whom the reported information relates prevail.

Here the Commission expressly recognises that the reporting obligations imposed by the U.S. Sarbanes-Oxley Act in the fields of accounting and auditing do represent a legitimate interest.

Information

a. Employees must be provided with clear information on the scope of application and purpose of the whistle-blowing system, both at collective and individual levels.

b. They must be informed of the type of reporting they should provide (which must consist of actual facts rather than mere rumour or conjecture) and on the reporting procedure (to whom, what, where, when, how, etc.).

c. The consequences of the reporting must also be described.

d. Only persons who are part of the organisation can report to, or be reported on, the whistle-blowing system.

No compulsory reporting

The use of the whistle-blowing system cannot be made compulsory and must be optional. The whistle-blowing system should complement other existing reporting channels and only be used where other reporting methods are not available.

Anonymous reporting only in restricted cases

The Commission indicated that, so far as possible, reports should be by identified whistleblowers and should not be made anonymously. The identity of the whistleblower must be kept confidential. Anonymous reporting should only be allowed in very restrictive cases.

Appointment of a complaints manager

An independent person must be nominated to deal with reports from the whistle-blowing system and to verify their accuracy. This "complaints manager" must operate under clear guidelines and be bound by strict confidentiality obligations. The whistle-blowing scheme must protect the whistleblower and the person to whom the reported information relates from any failure by the complaints manager.

No transfer outside the EEA

Any transfer of personal data received under the whistle-blowing system to a country outside the EEA must comply with the relevant provisions of the DPA. A transfer of this information to the company's headquarters outside the EEA will only be justified in very serious circumstances, such as where the reported facts could have an impact on the group as a whole.

Notification to the Privacy Commission

All whistle-blowing schemes must be notified to the Commission.

(The Commission's recommendation is broadly in line with the Article 29 Working Party's opinion).

  WDPR ISSN 1473-3579

Legislation & Guidance

Binding Corporate Rules: An Honest Appraisal from the U.K. Information Commissioner's Office

By Boris Wojtan, a solicitor at the U.K. Information Commissioner's Office, Wilmslow. The author may be contacted at boris.wojtan@ico.gsi.gov.uk

Ever since June 2003 when the Article 29 Working Party published its Working Paper 74 (WP74) on Binding Corporate Rules ("BCR"), data protection authorities (dpas) and companies have been optimistic that BCR could represent a 'win-win' situation: a win for the dpas in terms of increased or more effective data protection compliance and a win for companies in terms of reduced administrative burden. However, in the three and a half years or so that have elapsed since then, this optimism has become tainted with a growing sense of frustration by some at the slow rate of progress with the 'BCR project' and the high potential cost of seeking BCR approval.

This article sets out to give an honest appraisal of the challenges and solutions that lie ahead.

The first batch of applications – from GE, Philips and Daimler-Chrysler – have taken a very long time to process and have cost their respective corporate groups substantial amounts of money. Concerns have also been expressed about the lack of a harmonised approach between the dpas. Although some dpas are enthusiastic about BCR, they are experiencing difficulties with the compatibility of BCR with their national laws.

Under these circumstances it is perhaps understandable that CPOs and the like are having difficulty in getting their boards to sign off on a project that appears to be open-ended in terms of both time and money.

However, rather than throwing out the baby (the BCR project) with the bath water (the uncertainty and perceived cost of achieving BCR approval) it is preferable to take stock of the current status of BCR and how it is developing in order to form a realistic view of:

- How the BCR project will progress; and
- The resource implications and timescales for anyone considering BCR.

In order to gain this realistic view, it is necessary to:

- Remind ourselves why BCR is so desirable;
- Acknowledge the context and some of the factors that have prolonged the setting up of an efficient co-ordination procedure;
- Examine some of the challenges that we are facing as well as some of the solutions that are being discussed or implemented.

Armed with this realistic assessment, it is hoped that such intrepid CPOs will have enough ammunition to convince their boards that pursuing BCR is worth the effort.

A Reminder of the Benefits of BCR

In the real world ever increasing volumes of personal data are circulating the globe without much regard to international borders. The commercial pressures that underpin these trends in the way data flows should not be underestimated and whilst it is the dpas job to ensure that Articles 25 and 26 of the European Data Protection Directive 95/46 (the Directive) are adhered to and that individuals are protected, it is only sensible for dpas to pay heed to this dynamic.

The whole approach behind WP74 in providing an alternative to existing solutions like model contracts was to take existing global compliance practices such as internal codes as a starting point, that is to say: enable companies to comply in a way that suits their own compliance model.

Inspiration was drawn from various other forms of compliance regime such as corporate social responsibility reporting that have led multinational corporate groups to adopt global compliance strategies.

In this way a group of companies can simply adapt its existing global compliance model to incorporate data protection compliance rather than having to change radically its structure or business methods. This solution is, therefore, firmly rooted in the real world.

Not only will the harnessing of corporate codes in this way facilitate consistent data protection compliance for the group in the European Union, it may also provide the foundation of its global data protection strategy.

Although it is proving more elusive than was envisaged, we should not lose sight of the major advantage of a one-stop-shop: all dealings should be conducted through one lead dpa so that all bilateral discussions with other E.U. dpas regarding the group's BCRs fall away. This should translate into less time and money spent trying to satisfy numerous dpas on the same points of substance.

Finally, there is one argument in favour of BCR that has the potential to override all others and that is: *competitive advantage*.

By adopting a code of practice underpinned with policies and procedures that actually protect personal data rather than simply ticking a compliance box companies are engendering a sense of trust among their employees and customers.

Not only does this genuine privacy compliance make employees and customers feel good, it can actually help a company root out inefficiencies and open up new ideas.

This is entirely consistent with a general trend towards more transparent corporations that aspire – in much the same way as open source software attempts to do – to tap into the huge potential of the many and not the limited potential of the few.

All these factors can enhance reputation and increase competitive advantage.

From the point of view of the dpas, the benefits are equally irresistible: Instead of just receiving forms from a company, the dpa is getting a deeper insight into the way a company works and an assurance that protective measures are really adhered to in practice not just formally recorded. For example, the relevant training module and the accompanying controls to ensure that the appropriate staff have been trained can show that a company does equip its employees with the pertinent skills to recognise and deal with personal data issues.

Finally, there is a potential long-term benefit for dpas in terms of resource. It is hoped that the amount of work involved in approving BCR will cut down the amount of work that would otherwise have to be done (for example in approving standard contractual clauses). Also by encouraging data controllers to live and breathe data protection in practice where previously there was perhaps a focus on satisfying differing national formal requirements or putting a system of contracts in place, dpas should in theory have fewer complaints and prosecutions to deal with.

Whether or not this mini cost benefit analysis stands the test of time remains to be seen. Even if BCR does result in a net increase in the resources dpas needed, some would argue that the benefits in terms of better data protection awareness and compliance would easily justify such higher expenditure.

Acknowledging the Context

In order to understand how we got into a position where potential applicants have doubts about going ahead with a BCR, we have to go back to the beginning.

Mutual Recognition

At the time when WP74 was adopted it was felt that it was not possible to make use of mechanisms in the Directive for reaching collective decisions on an E.U. level (such as a Commission finding under Article 25(6) of the Directive).

There was not even scope to do the next best thing which is to recognise each other's decisions… so-called mutual recognition.

Indeed the only approach left open was for the dpas to sort it out amongst themselves under the auspices of the Article 29 Working Party (which is generally charged with the task of co-ordinating the efforts of all 25 dpas and ironing out the differences in implementation of the Directive).

The dpas would have to choose a lead dpa which would circulate a BCR application to the other dpas with a view to them all indicating informally and at the same time that they were satisfied with the adequacy of the safeguards in the proposed BCR. Depending on national requirements, after this informal agreement, each dpa would still have to process the application under its formal approval procedures.

It is this system that was proposed in WP74 and that found its way into WP107 which sets out the Co-operation Procedure. Whilst it is far from perfect, it was the only system that appeared to be available at the time.

Public Policy Concerns

If you put 25 CEOs of profit making companies together in a room to discuss a new idea – one which will enable each company involved to make more profit – agreement will be reached reasonably quickly as to how that extra value can be squeezed out of the idea and distributed amongst the participants.

If you put 25 dpas together in a room to discuss a new idea, the story is slightly different. Dpas (and regulators generally) have different concerns altogether.

Their primary concern is to regulate their sector well. To do this they have to take account of local culture and act in a way that is compatible with their national law. So, if a dpa says, "we cannot accept applications unless they are signed by a company established in our territory, because our national law says so", then that is a restriction other dpas have to take on board when they co-operate with that dpa. Dpas can not simply translate everything into monetary values, put the law to one side and 'take a commercial risk'.

Having said that, dpas *are* taking on a different form of risk by accepting the concept of BCR. Whilst they will continue to receive the same level of certainty and disclosure regarding processing that takes place within their jurisdiction, in respect of personal data being transferred outside the European Union the dpas are essentially accepting a broad set of promises that data controllers will behave in a certain way. For example, dpas considering a set of BCR are assured at the outset that the corporate group will inform data subjects of the purpose(s) for which the data will be processed and that the group will not use the data for other purposes. The dpas will not, however, know at the application stage of each and every possible future purpose. The parameters have to remain sufficiently flexible otherwise the system would be too rigid.

In embracing this kind of risk, it is perhaps not surprising that dpas will want to make sure that they and the data subjects are able to enforce the BCR after the approval and there are differences of opinion amongst dpas as to the appropriate level of certainty that is required.

For example, some dpas are adamant that each entity of a corporate group must be bound *in law* by the rules of the BCR, whereas others are prepared to accept that as long as each entity considers itself bound *in practice* that is sufficient.

The U.K. Information Commissioner's Office ("ICO") view is that a dpa will have the jurisdiction to intervene if a breach of the BCR (in relation to personal data originating in that Member State) comes to its attention and, ultimately, it would be able to withdraw the approval. As regards individual data subjects who are given the equivalent of third party beneficiary rights on the basis of a unilateral declaration (rather than in a contract), the legal position is not as clear. It is this office's expectation, however, that any national court in any E.U. Member State would be sufficiently sympathetic towards this attempt to grant jurisdiction to the data subject that it would accept jurisdiction.

However, these cultural and legal differences of opinion have to be respected and resolved together if we are to make BCR a success. We cannot simply translate them in to monetary values, calculate the costs and move on.

Resources

In an ideal world there would be mutual recognition and, let us say, three full time employees at each of the dpas dealing exclusively with setting up the BCR system and considering BCR applications.

However, in the real world there is something of a game of cat and mouse being played out. Companies are hesitant, because they want BCR to be fully established before they take the plunge. Dpas cannot justify creating long term posts when they do not know how many applications they will get. Planning the resource implications is particularly difficult at the early stages when volume numbers are low and some applicants withdraw half way through the project.

Without a steady flow of applications, the resources may not be put in place across the European Union to deal with BCR applications as effectively as possible. If all the potential applicant corporate groups wait for each other to go first, because the costs of getting approval will be lower in future, there is a risk that the BCR project loses momentum altogether.

Learning Curve

Before the dpas got together and agreed on the Co-Operation Procedure, it was difficult for dpas to know what to ask for or how to go about working together. Even after the Co-Operation Procedure was put in place there was (and perhaps still is) some hesitancy regarding the content. As yet we still do not know what makes a good application that will please everybody.

The Co-Operation Procedure can be fairly iterative in that the lead dpa has to work with the applicant to get the application into a state which it believes will be acceptable to the other dpas and the other dpas then have the chance to comment on the drafts. This can lead to several revision cycles or spin off into a side discussion.

It is only natural with the early applications that the dpas will either spend too much time requiring higher levels of protection that turn out not to have been necessary or assume a particular aspect to be sufficient only to find another dpa disagrees.

Over time and through shared experiences these sort of teething issues should resolve themselves.

Currently there are:

- four applications that are near the end of the Co-Operation Procedure
- four applications that are very advanced and that dpas have notified to each other in order to determine the lead dpa
- roughly a further 20-30 applications in respect of which applicants have had meetings with or shown documentation to dpas
- and many more expressions of interest.

Many applicants are telling dpas that they intend to wait until a few more applications complete the procedure.

Others are hesitating to involve dpas that have not yet dealt with applications, but this vicious circle is in the process of being broken. GE's application, for example was undertaken in two 'waves' that together cover each E.U. Member State. GE has gained approvals from almost all the first wave dpas and the second wave is in progress. So by now all E.U. dpas (apart from Romania and Bulgaria, who have only just joined the European Union) have considered at least one BCR application.

Challenges and Solutions

The factors described above give an idea of the context in which BCR is trying to emerge. However, whilst these factors may be difficult to change and mutual recognition might be a distant dream there are some more immediate initiatives that are taking shape now.

After taking stock of some of the difficulties that had been encountered with the GE approvals, the Article 29 Working Party recognised in April 2006 that the momentum had to be kept up. As well as charging the subgroup with the task of finding solutions, all the dpas present reconfirmed that the political will was there to do whatever is necessary to make BCR a viable mechanism for legitimising transfers of personal data outside the European Union. Unfortunately, this latter message did not receive quite as much attention as it deserved.

Later on in the year the Working Party began to focus its efforts on an initiative of the International Chamber of Commerce (ICC) to produce a standard application form that could be used in all E.U. jurisdictions and more recently on how best to streamline or standardise certain elements of the application.

Application Form

The possibility of an application form for BCR was discussed informally when dpas were working on the Model Checklist. At that time it was felt that such a form would be too prescriptive and in any event the Model Checklist gave a good overview of what was required. However, the experience of the GE application showed that an application form could have other advantages.

GE's application had been discussed by the same 10 or so dpas for quite some time and a point was reached where all dpas concerned were generally happy with it. It then transpired that in order to get the national approvals, national formalities had to be complied with. This led to yet more bilateral discussions and further delay.

It seemed obvious that if we could get the national formalities underway as soon as possible rather than waiting until the end we would save a lot of time. If the formalities could be consolidated into one form, even less effort would be wasted.

In September 2006 the Article 29 Working Party met to discuss the form proposed by the ICC. The Working Party was very positive about the ICC form and gave the subgroup the task of considering all the amendments to the form proposed by dpas and coming up with a final version to be approved by the full Article 29 Working Party as soon as possible.

At the time of writing the form is being voted upon in the Working Party's written voting procedure and, subject to any last minute tweaks, it looks likely that it will be approved. Although it is unlikely that all dpas will accept the ICC form in substitution for their own forms, there does seem to be a consensus that all national forms should be brought forward

and made available to applicants at the launch of the Co-Operation Procedure.

The form will quite sensibly have a detachable first part which will enable the dpa receiving the application to circulate it with a view to settling who should be the lead dpa. This first part will include all the relevant detail to identify the applicant company and the extent of the group as well as a brief description of:

- the justification of the choice of lead dpa (see Fig 1 for How to Choose the Lead dpa);
- the nature of the personal data being processed;
- the purpose for which it will be processed; and
- the flow of that data within the group in basic terms.

This high level information should give the dpas a quick grasp of the scope and extent of the application and will enable them to confirm or object to the choice of lead dpa more quickly. A more detailed description of the data flows is required in the second part.

Streamlining

It is a little ironic that one of BCRs greatest strengths has become one of its greatest weaknesses.

As mentioned above, the whole ethos of BCR was to allow corporations to approach data protection compliance in a way that suited them. To impose upon a group of companies a requirement that all their methods, procedures, models, policies etc demonstrating compliance with WP74 should be bound up in one all-encompassing document was deemed to be far too dogmatic. Much better, it was felt, to encourage diversity. Some companies might have one high level document enshrining all their core values with various policies flowing from that and supplemented by more practical guidance for appropriate employees. Other companies may have a more piecemeal approach with security, audit procedures, privacy policies etc all emerging independently from one another.

It was also felt that this flexibility would lead to genuine compliance throughout a group rather than a more formalistic tick-box attitude towards compliance.

All that was required from the dpas point of view was for all these strands of compliance to be brought together in an intelligible way. In order to help applicants, the dpas came up with the Model Checklist (WP108) and a requirement that a 'concise background document' be submitted summarising the various elements.

However, this has also proved to be a shortcoming. The companies want to know what the dpas are looking for and the dpas can not tell them because it is up to the companies to demonstrate how they comply. (See Fig. 2 for What to Submit)

Not only is this leading to hesitation all-round, it also makes the job of evaluating the content of submissions much harder.

Whilst the application form might help in this regard, there are undoubtedly more specific areas that could be elaborated into forms of declaration or some other such standard and informal discussions are underway to explore this. If the discussions are fruitful it is probable that such efforts to standardise will find their way on to an Article 29 Working Party agenda in the not too distant future. It is also possible for interested business groups or academic volunteers to undertake projects of this nature for submission to the Article 29 Working Party.

Mutual Confidence

Whilst formal mutual recognition may still be a long way off, there is nothing to stop dpas developing their sense of trust in each other.

One of the difficulties that can occur with the BCR process is that dpas seek to impose elements of their national data protection regime on the applicants. This is a perfectly understandable instinct, but taken to its logical conclusion would lead to gold plated super-protection and possibly even expose some conflict between the various national laws. Such strict requirements would frustrate the rationale of BCR and it is questionable whether are really necessary.

It is worth reminding ourselves that BCR is a means of "adducing adequate safeguards" under Article 26(2) of the Directive and not a complete notification of processing activities. It is intended to demonstrate to the dpas in countries from which personal data are exported, that the same high level of protection will apply to those data throughout the group.

The confusion arises because dpas considering a BCR application will inevitably be looking at a broad range of protection measures. When faced with, for example, a company's data retention policy, it is easy for a dpa to think of the standard that applies in its own country. Instead it should ask itself whether that standard is good enough when combined with all the other protection mechanisms in the BCR to amount to "adequate safeguards" for the purpose of the Directive.

There is little doubt that such requirements will decline as time goes on and as dpas work more closely together on BCR applications.

Applicants will also take heart from public pronouncements such as that of the Dutch dpa recently which said that they would use their power to ask for clarification and specification only very sparingly in relation to applications that come to them from other lead dpas.

This sort of mutual confidence will greatly speed up the application process and is key to the success of BCR.

Reconsider the Directive

Some ideas involve a more radical change of tack. For example, some people are suggesting it may be possible for the Commission to make decisions on BCR on the basis of Article 26(4) whilst others drawn to the possibility of codes of conduct under Article 27 as a means of approving BCR collectively.

Third Party Certification

Another idea worth considering is the use of third party certification bodies to help boost the quantity and quality of approvals.

Although it is not yet quite clear how such bodies could best be engaged there are some clear benefits.

The accreditation can be seen as a sort of branded logo or badge of honour to show to the outside world how seriously a company takes its privacy obligations.

It could also be of great assistance in the approvals process. Although the final decision would always be at the discretion of the dpa, the accreditation work carried out by such third

parties could save the dpas a lot of work. Naturally, in order to implement such a system, clear objective criteria would need to be defined, but such an exercise would not be dissimilar to the 'streamlining' exercise described above.

Similar schemes have been used in relation to the U.S. Safe Harbour regime and apparently dpas in ASEAN are considering such a move for their equivalent of BCR.

Third parties could certainly provide useful assistance in monitoring whether or not a company is complying with its obligations under the BCR and they could facilitate dispute resolution mechanisms between data subjects and the company.

Website

Another way in which the process may be improved is if all the dpas set up a dedicated joint website to which all the parties would have access to ensure greater transparency. This could include all the obvious resources, but also all the formal application forms procedures that an applicant would have to go through at a national level could be brought together here.

Conclusion

The BCR project got off to a slow start with disproportionately high costs for the first few applicants. There has been a period of near stasis whilst dpas adjust to the new approach and potential applicants play a waiting game.

The time it takes to complete the approvals process should already be much shorter than our experiences with GE, Philips and Daimler-Chrysler would imply (although this is difficult to say for certain until more applications get through the process). With the introduction of the application form and other streamlining efforts the time should be reduced even further in another year or so.

Effort expended by applicants in bilateral discussions with dpas and repeated revision cycles should also be reduced in parallel with the length of the process.

In the short term the input required by applicants is likely to remain high but nowhere near as high as for the first three applicants whereas in the medium term there will be greater certainty and much reduced costs.

However, it should be stressed that unless a significant number of companies are willing to press ahead now to help pioneer the BCR project momentum will be lost. Without the applications the dpas can not plan their resources effectively.

The alternatives to BCR are often either inappropriate or burdensome: Safe Harbour is only relevant if you are transferring to the United States; standard contractual clauses are cumbersome when you have numerous group companies and are often used in a tick-box way; and the U.K. Information Commissioners Office's view that a data controller can assess adequacy itself is not generally shared across the European Union.

BCR represents a golden opportunity to try a new approach. There are tangible benefits for industry and for good data protection practice generally. We can either embrace this opportunity with all its imperfections and try to make it work or we can shrug our shoulders and make do with the existing somewhat inflexible solutions for transfers of data outside the European Union.

In many ways there is nothing to lose: if for some reason the BCR project collapsed and an applicant was left with unapproved BCR, the time and effort it will have put into those BCR will not have been lost. By the very definition of BCR, if an applicant adopts BCR in its group, it is establishing good data protection practices that will not only help with data protection compliance the world over, but also demonstrate to the world that the applicant takes privacy seriously.

Hopefully this article has demonstrated that data protection authorities are aware of the frustrations of potential applicants and are aware of the causes of those frustrations. Whilst there are some factors contributing to the delay that are hard to overcome, there are others that can be acted upon now and the dpas *are* acting to improve the system for the benefit of all.

Figure 1

What to Submit

The lead authority needs to see:

- A separate document containing:
  - Details of the applicant company and the scope of the group
  - The justification of choice of lead authority
  - A brief description of the nature of personal data, the purposes of processing and where it usually goes from and to

This separate paper can then be used to circulate to other dpas

- The BCR comprising any high level documentation setting out the principles, policies or procedures relating to data protection. (These 'rules' may be incorporated in a single document or dispersed in various documents. It depends on how the group feels it can best police its own code.)
- Supporting information. (This could be anything from excerpts from standard contracts to slide shots of training programmes to show how the group handles personal data. The applicant may also be asked to answer specific questions.)
- A concise background document. (This is not part of the group's BCR as such, but acts as a guide for all the dpas considering the application.)

If the Application Form gains approval from the Article 29 Working Party, it is likely that it will replace the first and last items above. However, there is a difference in style and it is possible that applicants will want to retain the ability to make representations alongside the application form rather than in it.

How to Choose Lead Authority

The Co-Operation Procedure in WP107 sets out some useful criteria for choosing the most appropriate lead authority:

- the location of the group's European headquarters;
- the location of the company within the group with delegated data protection responsibilities;
- the location of the company which is best placed (in terms of management function, administrative burden etc) to deal with the application and to enforce the binding corporate rules in the group;
- the place where most decisions in terms of the purposes and the means of the processing are taken; and
- the member states within the EU from which most transfers outside the EEA will take place.

There is a degree of flexibility in how these are applied. Applicants should consider all of the factors and select a lead authority on balance. If in doubt, remember you can always discuss your thoughts with one of the data protection authorities.

Although priority is to be given to the first criterion, this will only apply where the ultimate HQ is in the EU. If there compelling reasons to choose a different authority, because, for example, all the management functions are actually based in another EU Member State then raise the issue with both authorities.

Data Protection and Intellectual Property: Document Number 104 from the Article 29 Working Party[1]

By Leonardo Cervera Navas,[2] Administrator, DG Internal Market and Services, Copyright unit, European Comission, Brussels. The author may be contacted at Leonardo.Cervera-Navas@ec.europa.eu

The interaction between data protection and intellectual property is a complicated matter, in particular for those who approach this issue for the first time. Therefore, I have been reflecting on the best way of providing meaningful introductory explanations, which will also be of interest to those who are more familiar with this subject.

To the best of my knowledge, the only official document (although soft law) ever written at European level on this interaction is document number 104 of the Article 29 Working Party.[3] Of course it is always difficult to assess to what extent this document has received the attention of experts. A simple search on the Internet does not reveal any significant results.

Therefore in the hope that these pages will make a very small but meaningful contribution to this matter, in this article I will consider the salient aspects of this working document and review the reactions to this document from: the copyright industry, internet service providers, authors' collecting societies, other rights-holders and academics.

Before reviewing the substance of this working document, let me first set-out the most relevant European legislation on this issue:

a. Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[4]
b. Directive 2002/58/EC of the European Parliament and of the Council of July 12, 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)[5]
c. Directive 2000/31/EC of the European Parliament and of the Council of June 8, 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') [6]
d. Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (Copyright in the Information Society)[7]
e. Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ L 157, 30.4.2004)[8]

In this *acquis*,[9] there are four provisions which are particularly relevant for this relationship between intellectual property and privacy:

1. Article 5.1 of Directive 2000/31/EC excludes from the scope of application of the e-commerce Directive any issues regulated by Directives 95/46/EC and 2002/58/EC (Data Protection).
2. Article 15 of the same Directive states that a general obligation should not be imposed on Internet service providers to carry out active investigations of illicit acts.
3. Recital 57 of Directive 2001/29/EC provides that: Any such rights-management information systems referred to above may (depending on their design) at the same time process personal data about the consumption patterns of protected subject-matter by individuals and allow shadowing of their on-line behaviour. These technical means in their technical functions, should incorporate privacy safeguards in accordance with Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals, with regard to the processing of personal data and the free movement of such data.
4. Article 8 of Directive 2004/48/EC empowers right holders to request and obtain information from third parties, on persons responsible for, or suspected of intellectual property violations. Although with full respect of the data protection legislation (see third paragraph of this provision).

The Main Data Protection Issues for the Working Document in Relation to Intellectual Property Rights[10]

The working document expresses on the one hand, the concerns of the European data protection authorities, due to the invasive nature (from the data protection perspective) of many DRMs (*Digital Rights Management Systems)* While on the other hand, it refers to the limitations of sharing information for enforcement of intellectual property rights as a result of the European legislation on personal data protection.

The Article 29 Working Party refers to the fact that Article 2.3 of Directive 2004/48/EC (enforcement Directive) clearly reflects that the enforcement Directive does not prejudice the data protection *acquis* and sets out the following main data protection principles:

a. The necessity principle: those who want to transact anonymously should have the right to do so. Unique identifiers, used by some right holders might be problematic from this point of view.

b. The transparency principle or information principle: data subjects should at least be informed of the identity of the data controller, the purpose of the processing, the recipient of the data and the rights of access and rectification.
c. The compatibility principle: the information collected from individuals may only be processed for purposes compatible with those declared at the time of the collection, and
d. Limited retention periods: data should not be kept longer than necessary and it should subsequently be destroyed.

The working document then reviews the processing of personal data for investigation, or enforcement purposes, in connection with violations of intellectual property rights. The Article 29 Working Party mentions that databases set up for a given purpose (*e.g.,* billing or technical matters) cannot be used for incompatible purposes such as enforcement of intellectual property rights.

The European data protection authorities also stressed in this document (that as provided for in Article 15 of the e-commerce Directive) Internet service providers do not have a general obligation to control and co-operate with holders of intellectual property rights. Finally, the data protection group also reviewed the issue of processing of judicial data in such a way, (as explained later on) that has been strongly criticised by representatives of copyright holders.

The working document concludes by re-iterating the concerns of the European data protection authorities. Namely that the use of DRM's may create differences between the on-line and the off-line world, and urges holders of intellectual property rights to be transparent and to use privacy-friendly technologies.

The Copyright Industry's Response to the Working Document

Document number 104, adopted in January 2005, was subject to a public consultation for two months. The answers received (36) were published[11] but so far, there does not seem to be a summary of them or a list of any proposed changes to the working document. This might indicate that the issue is no longer a priority for the Article 29 Working Party.

In general, the answer provided by the copyright industry and collecting societies was very negative, although the tone of stakeholders in the area of copyright is generally more aggressive than the tone employed by stakeholders in the data protection field.

Conversely, the answers given by the Internet service providers and telecommunication companies[12] were very positive (even advocating a more restrictive approach, *e.g.,* Telecom Italy's comments as regards the international transfer of personal data).[13] This clearly indicates that the data protection debate is being orchestrated by stakeholders, to a great extent.

It would take too long to make a comprehensive summary of all the comments made. Therefore, please note that the summary below is merely illustrative and does not accurately reflect all comments or all associations or companies having subscribed to them.

The Criticism from IFPI

The strongest reaction to the document came from the IFPI (*International Federation of Phonogram Industries*).[14] This association denounced the Article 29 Working Party, stating that the Working party did not seem to have understood properly the role of DRM's and the uses which the copyright industry is making of them.[15]

Concerning the issue of the right of users to remain anonymous, phonogram producers stated that such a right does not always exist in the off-line world, and mentioned that users remain free to choose whether to use the service or not.

IFPI also disagreed with the Article 29 Working Party on the negative views expressed as regards the 'unique identifiers', given that most of them would not serve the purpose of identifying people by way of the copyright product itself.

Nevertheless, it is on the issue of enforcement where record companies seem to disagree most with the data protection authorities. For IFPI it is not at all clear at that IP addresses (internet protocol addresses) can be considered personal data and therefore they question the application of data protection legislation to any processing. Besides, the reference to the *Verizon* affair as an example of a prohibition to use traffic data resulting from peer-to-peer networks, would always be misleading in the opinion of the phonogram producers, as the issue discussed in this American case would not be representative of the issues and practices relevant to the European Union.

IFPI concluded its criticism of the working document by stating that data protection would be used in bad faith to give coverage to violations of intellectual property rights and that, in view of the huge scale of piracy, the legitimate interests of holders of intellectual property rights to stop these practices should prevail over data protection rights.[16]

The Finnish Confederation of Industries and the ICMP (International Confederation of Music Publishers) also adopted a similar approach in their responses and drew the attention of the Article 29 Working Party to the fact that current business models of creation and distribution of music require a lot of processing of personal data. This relates to both that of the consumers, and of the artists themselves.

The Comments of the MPAA

The Motion Picture Association of America, is the industry association of the major film producers. While using a more moderate tone, they substantially agreed with the concerns expressed by IFPI. MPAA denounced the fact that data protection legislation would be used by hackers and pirates to obtain impunity from outright violations of intellectual property rights.[17]

The association of film producers expressed regret that the Article 29 Working Party did not seem to fully understand

the important role that DRM's play in the information society, by offering exciting possibilities to citizens. Which explains why these new technologies are being promoted by national and international administrations.

Film producers also disagree with the interpretations of the data protection group on the complex issue of judicial data. In the MPAA´s view…any IP addresses, or any other data collected and processed by copyright-holders during an investigation to obtain evidence of intellectual property violations, cannot be deemed judicial data. Therefore such data would not benefit from the "additional safeguards" foreseen by the Data Protection Directive. In the MPAA´s view (a view shared by most comments in the public consultation) judicial data are those originating directly from judicial procedures,[18] as any other interpretation would have a negative effect on the rights of holders of copyright to investigate and defend themselves from violations of intellectual property rights.

Other Comments from the Copyright Industry

British Music Rights, the association representing composers, producers and collecting societies in the United Kingdom asked the Article 29 Working Party to reconsider their approach and show a more flexible and understanding attitude. For example, in relation to the transparency principle and the right to remain anonymous. Concerning the processing of personal data for enforcement purposes, BMR proposed the setting up of special entities, which in agreement with the data protection authorities would benefit from special privileges to process personal data.[19]

The digital watermaking association criticised the negative approach of the working document in relation to the unique identifiers issue, which in their opinion is mainly used to identify content and only rarely people.

GESAC, the European association of collecting societies, found the approach in document 104 too restrictive and too negative as regards DRM's. Which in their view ultimately benefit citizens by allowing for enormous flexibility and innovative uses of copyright content.

Four associations of the publishing sector also submitted comments to the working document: ENPA (*The European Newspapers Publisher Association)*, EPC *(The European Publishers Council)*, that is, the association grouping the views of the most important European media groups, EFP (European Federation of Publishers), the association of book publishers and PPA (*Periodical Publishers Association)*, the association of British publishers of journals.

In general, publishers criticised the uncertainties surrounding the relationship between intellectual property legislation and data protection legislation. In their comments, they complained about the use of expressions such as "without prejudice to data protection legislation" in the copyright *acquis.* In their opinion, this would have opened up too many issues. Nevertheless, publishers appear to be against legislative changes preferring to deal with the current situation as it is (better the devil you know...)

Comments from the Academic World

Two answers received from the world of academia deserve recognition in my view, the response from CRID[20] (Centre de Recherches Informatique et Droit) in Europe, and the contribution from EPIC[21] (Electronic Privacy Information Centre).

EPIC referred to the constitutional character of data protection in Europe, and urged copyright industries to develop and implement DRM's that do not process personal data. EPIC also denounced the temptation within some companies to collect more personal data than strictly necessary for the provision of the service, with little transparency, and on the basis of a contract of adhesion of questionable legality. EPIC also mentioned that the only lawful consent is informed consent, and expressed serious doubts that data collected for commercial purposes could be re-used for enforcement purposes, on the basis of vague clauses contained in contracts of adhesion.

Finally, adopting a similar line to the Article 29 Working Party, EPIC recommended the development of PETs *(Privacy Enhancing Technologies)* which would be considered a competitive advantage for those companies investing in this area.

CRID positioned itself in the middle ground, between the interests of data protection and the interests of intellectual property. For example, CRID reflected on whether the processing of personal data for enforcement purposes could not be considered as one of the legitimate purposes provided for in Article 7.f of the Data Protection Directive. That is, processing of personal data necessary to safeguard a legitimate interest of the data controller or the recipient of the data.

This Belgian research centre also recommended a realistic approach to the issue of anonymity in the Internet. As they felt that this might be something very difficult to achieve by technical means and even incompatible with the provision of some services.

CRID shared the doubts expressed by many others, in relation to the unusual interpretation of the issue of judicial data contained in the document, and reviewed the right of information of Article 8 of Directive 2004/48/EC (Enforcement). In this respect CRID makes an interesting differentiation between those stakeholders who obtain a commercial gain (*e.g.,* Internet Service Providers) and those who do not (*e.g.,* a University). On the basis of this distinction, CRID concludes that in the presence of a possible violation of intellectual property rights, an Internet service provider would be obliged to provide personal information to the right holders, while a University may refuse to provide personal information regarding its students.

Final Considerations

So far, the relationship between data protection and intellectual property in the European Union has been peaceful. In my opinion there are two reasons that justify this situation:

First of all, contrary to the initial expectations, there have been not many actions against users of P2P networks. Most commentators are of the view that the copyright industry would be afraid of taking more actions against users. Not because they fear that the evidence collected might be declared illegal on data protection grounds, but because they are afraid that the image of their corporations may be fatally harmed if they are associated with court cases against students and teenagers liable for actions that most people (including judges) would not consider to be malevolent.[22]

Secondly, because the implementation of Directive 2004/48/EC on enforcement, (the legal text that gives clearer rights to copyright industries to request and obtain personal information), is still ongoing in many member states. Furthermore, potential conflict with data protection legislation has not been yet tested in courts and tribunals.

There are however, some clear indications that this peaceful relationship between data protection and intellectual property might not be that peaceful in the future. Because of my expertise on both topics, I am frequently asked the question of who will prevail eventually.

I must say that at this very moment I do not have sufficient information to risk a clear answer. My experience over the last years indicates that data protection legislation benefits from the enormous sympathy of the judges and public authorities who may be called to rule on this issue. At the same time, nobody should lose sight of the fact that the copyright industry is fighting a battle of survival against this phenomenon usually called "piracy" and that it will do whatever is necessary to win the day or to have the legislation changed, if necessary.

Therefore, sharing this personal sympathy towards the development of E.U. data protection law, and being conscious of the important interests at stake, all I can say at this moment is: *"may the force be with you"*[23] Data Protection Directive.

1 A similar article in Spanish was recently published in the electronic magazine of the Madrid Region data protection authority (Spain): *www.datospersonales.org*

2 All opinions expressed in this article are strictly personal and do not represent the views of the European Commission. Leonardo Cervera works as an administrator in the copyright unit of the European Commission. From September 1999 until February 2005, he worked in the data protection unit of the European Commission.

3 The Article 29 Working Party is the meeting of representatives of European data protection authorities set up by Article 29 of Directive 95/46/EC.

4 *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML*

5 *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML*

6 *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:ES:NOT*

7 *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001L0029:EN:HTML*

8 *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004L0048R(01):EN:NOT*

9 The term 'Acquis' is used in E.U. law to refer to the total body of E.U. law accumulated so far http://en.wikipedia.org/wiki/acquis

10 Document available in English, French and German in the following address: *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp104_en.pdf*

11 *http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/consultations/intellectual_property_rights_en.htm*

12 See at this regard the reaction of EUROISP (European Association of Internet Service Providers), ETNO (European Telecommunications Network Operators) and Telecom Italy.

13 *http://ec.europa.eu/justice_home/fsj/privacy/docs/intellectual_property_rights/telecom_italia_group_en.pdf*

14 See for example the very first paragraph of their answer: *(...) "The working document (…) in its present form includes a number of factual mistakes, misunderstandings and legally disputable conclusions"*

15 *http://ec.europa.eu/justice_home/fsj/privacy/docs/intellectual_property_rights/ifpi_en.pdf*

16 "Given that the vast bulk of music files on the Internet are illegal, and that right holders and their agents only collect IP addresses of computers internationally put on the Internet by users offering illegal material, it is difficult to see how the interests of the fundamental rights and freedoms of the person making infringing files available on the Internet could override the copyright enforcement interests of right holders (…) A balancing of these rights against the right to privacy of persons who are manifestly infringing right holders' rights to the detriment of such a wide grouping of interests can surely not result in it being impossible for right holders to effectively take any action against them".

17 See page 2 of MPAA comments, second paragraph: "(…) We would like to draw the attention of the Working Party to what we see as a worrying trend toward the use of legitimate privacy rules as a cover-up for illegal on-line activities, such as IP infringements, hacking, hate crimes, phishing/other forms of fraud, child pornography, cyber-squatting, etc…"

18 See on this issue, page 5, second paragraph: "Article 8.5 explicitly refers to data on *offences* (as opposed to allegations, charges, or the suspicion of criminality), *criminal convictions* and *registers* of criminal convictions. This can extend to other final results of formal adjudicative process: *administrative sanctions* and *judgments* in civil cases. The legislative intent behind this provision of the Directive is quite clear – for data to be *judicial data*, it must arise directly from judicial proceedings.

19 See page 4, forth section: *"under an approval system, certain private and public bodies could quality for a special status regarding the handling of data".*

20 *http://ec.europa.eu/justice_home/fsj/privacy/docs/intellectual_property_rights/crid_en.pdf*

21 *http://ec.europa.eu/justice_home/fsj/privacy/docs/intellectual_property_rights/epic_en.pdf*

22 The Spanish judge Paz Aldecoa has recently appeared in all newspapers´ headlines when she did not find guilty a user of P2P networks on the consideration that all the music and movies copied by this person were private copies and there was no commercial interest: *"Ni mediaba precio ni aparecían otras contraprestaciones que la propia de compartir entre diversos usuarios el material del que disponían. Y, a juicio de esta juzgadora, ello entra en conexión con la posibilidad que el artículo 31 de la Ley de Propiedad Intelectual establece de obtener copias para uso privado sin autorización del autor; sin que se pueda entender concurrente ese ánimo de obtener un beneficio ilícito". "Sin ánimo de lucro, los hechos no constituyen una infracción merecedora de sanción penal".*

23 Popular expression of the Star Wars saga used to wish success in the forthcoming battle.

UK Government announces tougher penalties for data protection offences

By Gary Brooks who is a Senior Associate at Berwin Leighton Paisner LLP. The author can be contacted at gary.brooks@blplaw.com

On 7th February 2007, the UK Government announced plans to make penalties for the trade and misuse of personal data more severe, by introducing a maximum two-year jail term for offenders.

This significant new measure is a direct result of the Government and the data protection regulator's increasing concern about the apparent growth in the illegal trade of personal data, in particular "blagging". "Blagging" is a practice whereby an individual contacts an organisation (typically by telephone) pretending to be someone else (for example the Inland Revenue) in order to extract personal data by deception. The acquired data is then sold on, with buyers of such data typically being journalists, unscrupulous direct marketers, private investigators or debt collection agencies. The Information Commissioner (the UK data protection regulator) recently published a league table of those newspapers and magazines who have unlawfully bought people's personal information in search of a story.

This move comes in response to a public consultation on increasing penalties for deliberate and wilful misuse of personal data, which resulted from two presentations by the Information Commissioner to Parliament entitled 'What Price Privacy?'[1] And 'What Price Privacy Now?'[2] This development is part of the Government's overall strategy for increased data sharing to deliver better public services to individuals, which is going to be a key theme in 2007 on the privacy and data protection front in the UK.

The Commissioner carried out a number of prosecutions in 2006 against blaggers. However, current penalties consisting of a fine in the Data Protection Act 1998 ("DPA") have not provided a sufficiently strong deterrent and have not been viewed as strict enough.

It is a criminal offence in section 55 of the DPA to knowingly or recklessly obtain, disclose or procure the disclosure of personal data without the consent of the organisation holding the data. It is a separate offence to sell or offer to sell on that illegally acquired data.

Currently, the DPA provides for the following penalties: on summary conviction, a fine not exceeding £5,000 and on conviction on indictment, an unlimited fine.

The Government intends to amend the DPA to make the following convictions available to the Courts, in addition to the current fines:

a. on summary conviction, up to six months imprisonment (increased to twelve months imprisonment in England and Wales when part of the Criminal Justice Act 2003 comes into force); and
b. on conviction on indictment, up to *two years imprisonment*.

This announcement is clear evidence of a tougher approach to the enforcement of data protection law, which is to be welcomed given that the DPA and its enforcement regime have previously been criticised for lacking teeth and for not providing organisations with any real incentive to achieve compliance.

What does this mean for your own data protection compliance?

This development should at least serve as a reminder to all businesses of the danger posed by blaggers. The seventh principle of the DPA requires organisations to have sufficient data security measures in place to prevent unlawful access to personal data that they hold. If blaggers are able to obtain personal information from your organisation through simple communication such as a phone call, this could be viewed as a data protection breach on your part, unless you can show that you have adequate security procedures and staff training in place to prevent such activity.

Buyers of data need also to beware. All data controllers must ensure that they acquire personal data from third parties lawfully and if you are going to acquire data from third parties (e.g. for marketing prospective customers), you should seek assurances that the seller can disclose this information to you without breaching the DPA. If you procure personal information via a third party (who obtains such data by illicit methods), *e.g.*, an unscrupulous private investigator, you are potentially committing an offence under the DPA, which if successfully prosecuted, could lead to considerable embarrassment for your organisation as well as the criminal sanctions mentioned above.

1 See *www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/what_price_privacy.pdf*
2 See *www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/ico-wppnow-0602.pdf*

News

Irish privacy law poses threat to press freedom

By Dr Chris Pounder of Pinsent Masons Solicitors, London. The author may be contacted at chris.pounder@pinsentmasons.com

In an open letter to the Irish Prime Minister, Bertie Ahern, and Justice Minister Michael McDowel, the World Association of Newspapers and the World Editors Forum have protested to the Irish government against proposed privacy legislation.

A new law, the letter states, conflicts with press freedom in Ireland and would "inhibit the way newspapers carry out their legitimate and important function in society". The organisations are "seriously concerned that the Privacy Bill poses a significant threat to press freedom and would, if enacted, make unlawful the publication of much material that is clearly in the public interest".

The press organisations have called on the Irish Government to withdraw its Privacy Bill and adopt an industry-backed proposal to establish a press ombudsman and press council. This would establish a very similar regime to the Press Complaints Commission in the United Kingdom. "We ask that the press be allowed to demonstrate that a self-regulatory system can promote high journalistic standards and deliver

  WDPR ISSN 1473-3579

effective redress for complainants, while protecting press freedom, as is the case in most of Europe," the letter said.

According to the statement, the proposed Privacy Bill would restrict publication of information in numerous publicly available documents, enable individuals to secure court orders in secret to prevent publication of certain materials, prevent "watching, besetting or following" even in cases where journalists believe someone may be guilty of a serious crime, and would allow individuals to secure injunctions to prevent pursuit by journalists as soon as they are aware they are being investigated.

The Irish Government published at the same time as its Privacy Bill, legislation which would protect the press from actions for defamation. For some reason, the World Association of Newspapers and the World Editors Forum have not protested at the Defamation Bill. In practice we do not think the Irish Privacy Bill will make it to the statute book until 2008 at the very earliest (if ever). The reason is that there has to be a General Election in Ireland next year, and no sane politician would contemplate legislation which would ensure that every newspaper in Ireland would be telling their readers to vote for someone else.

Obligations Under Franchise Agreement and Data Processing Requirements – Alleged Conflict

Written by Andrew Clay, Hammonds, Leeds. The author can be contacted at andrew.clay@hammonds.com

Grow With Us Ltd v Green Thumb (UK) Ltd 2006 EWCA Civ 1201 (27 July 2006). The Court of Appeal has dismissed the appeal by Grow With Us, the franchisee under a franchise agreement with a lawn treatment company called Green Thumb, against the decision of His Honour Judge Seymour QC, that its failure to reach minimum performance targets precluded it from renewing the franchise agreement. As such, the court did not need to deal with the franchisee's arguments that it was precluded from complying with one of its obligations under the agreement because this would have contravened the Data Protection Act 1998. Nonetheless, the court considers those arguments and in endorsing the judge's view provides valuable guidance, albeit obiter, on the application of the fair processing requirements and respective responsibilities of the parties in the context of contractual obligations to transfer personal customer data between parties to a franchise agreement.

Background

Grow With Us, the franchisee, sought a mandatory injunction requiring Green Thumb, the franchisor to perform its obligation under their franchise agreement to extend the terms of the agreement for a further seven years. Green Thumb argued amongst other things that they were not obliged to do so because Grow With Us was in breach of the agreement by failing to supply it with details of the names and addresses of Grow With Us customers. Grow With Us argued that the breach was excused by virtue of the fact that compliance with the contractual obligation would have amounted to a breach of the 1998 Act. At first instance, Judge Seymour found in favour of Green Thumb, the franchisor. Grow With Us appealed.

The issues

The Court of Appeal dismissed the appeal on the basis of the franchisor's other contentions that Grow with Us had failed to satisfy minimum performance targets. Buxton LJ nevertheless went on to consider the data protection arguments. These related specifically to Clause 4.1.20.2 of the agreement which obliged Grow With Us "to supply to the Franchisor by electronic means (if required by the Franchisor) monthly sales reports and other information in the form stipulated by the Franchisor in the Manual concerning the Business". By clause 5.1.34, Grow With Us were to keep a list of actual and potential customers of the business and supply a copy of it to Green Thumb on request. They persistently refused to transfer those details. Green Thumb sought to terminate the franchise on the basis of the breach of this and other requirements under the agreement. Their case on appeal was therefore that Grow With Us as a result of those breaches was not entitled to seek a renewal.

Court of Appeal

Like the judge, Buxton LJ would have dismissed the franchisee's case that to transfer the file would have constituted data protection breaches. For a start the whole argument was "bedevilled" by the assertion or assumption that once the Data Protection Act issues had been raised, it was in some way for the franchisor to show that the Act was not infringed. Rejecting that view, Buxton LJ agreed with the judge that "once it was accepted that the franchisee had failed to provide to the franchisor information which it was contractually bound to provide, the evidential burden of proving that there was an excuse for that failure passed to the franchisee".

Nevertheless Buxton LJ noted that it was common ground that the names and addresses of customers and possibly some other information about them, for instance the key code for their front doors, were personal data for the purposes of the Act, and that electronic transfer of that data to the franchisor would constitute processing of that data under the Act.

Fair processing

The franchisee's first submission was that the transfer of such data would not be fair processing under Part 1 of Schedule 2 to the Act, which provides that personal data shall be processed fairly and lawfully and in particular shall not be processed unless at least one of the conditions in Schedule 2 is met. In this respect Grow With Us argued that the transfer of the data would not amount to fair and lawful processing in accordance with the first data protection principle because they did not have sufficient information to be able to comply with the requirement under the Act that, where data is obtained from a data subject, the data controller ensures, as far as practicable, that the data subject is provided with information regarding the purpose for which the data is intended to be processed. Grow With Us contended that the purpose had not been made clear to them.

Buxton LJ rejected this argument on the basis that, at this stage of the process, it was Grow With Us that was the data controller. The responsibilities were therefore the franchisee's and Green Thumb did not become the data controller until the data was transferred. Thus the complaint that a customer was not properly informed of the purpose for which the data was to be used in the first instance seemed "to beat the air".

Buxton LJ also rejected a fair processing argument based on the contention that the franchisor's statement of its data protection policy on a promotional document was insufficient or misleading. The statement read as follows:

Green Thumb (UK) Ltd and its franchisees take the issue of protecting your personal information seriously and would be grateful if you would take the time to read the following information about our use of your personal information. We will use your personal information to provide and enhance our services to you; deal with enquiries, administration, security and market research.

The nub of the franchisee's complaint was that the statement did not say in terms that the information was to be used by the franchisor for the purpose for which the franchisee said it principally required it. As far as the judge was concerned, however, the registration requirements of the 1998 Act did not require the applicant for registration to set out exhaustively, as opposed to sufficiently to give an understanding of the general nature of the processing intended, what it proposed to do with the data obtained. Agreeing with that sentiment, Buxton LJ dismissed the franchisee's contentions, adding that in any event if the Grow With Us the franchisee was worried about this clause, they could themselves have told the customer in more detail how the information was to be used.

Schedule 2 conditions

The franchisee's next complaint was that Schedule 2 of the Act had not been satisfied. This provides that in order for personal data to be processed fairly one or a series of conditions must be met. The complaint related to two conditions, the first relating to whether the data subject had given his consent to the processing. Grow With Us argued that they were so tightly bound by the terms of the franchise agreement that they could not do anything that was not provided for in the agreement and the company Manual, not even ask customers for consent to transfer their information, without the consent of the franchisor. Buxton LJ could see nothing in the terms of the franchise agreement, however, to suggest that the franchisor could not have been approached for its consent. Accordingly, there was no good reason in terms of condition 1, customer consent, for the franchisee's failure to transfer to the data file.

That being so, the further contention relating to condition 6, that processing was necessary for legitimate interests of the franchisor, became academic. Nevertheless, Buxton LJ endorsed the judge's view that Green Thumb might well have a legitimate interest in receiving the information as to the names and addresses of the franchisee's customers, and that it was not obvious that passing on that information would cause prejudice to the rights and freedoms of the customers. The provision of customer information was particularly important for Green Thumb for a number of reasons, including to monitor customer turnover accurately and provide necessary assistance and advice to the franchisee, and also to audit turnover and ensure correct returns without access to the data.

Comment

The Court of Appeal was not actually obliged to deal with the data protection issues in detail. The fact that it did suggests that it felt it necessary to disabuse commercial parties of the notion that the 1998 Act can be used creatively to avoid obligations under a contract. The standard arrangements between parties to a franchise provided an excellent scenario within which to test issues raised under the fair processing requirements of the Act in relation to the sharing of customer data. The court considered, as did the judge at first instance, the practical implications of some of the franchisee's arguments and seeing that for practical purposes the franchisee could itself resolve some of those issues, for example by seeking consent from customers itself or at least asking the franchisor for permission to do so, was not prepared to allow Grow With Us to hide their contractual failings behind either their own or Green Thumb's duties under the 1998 Act.

Online Shopping Under the E.U. Microscope

By Vanessa Barnett who is a senior associate at Berwin Leighton Paisner LLP. The author may be contacted at vanessa.barnett@blplaw.com

In a bold move in her first press conference yesterday, the new E.U. Commissioner for Consumer Affairs, Meglena Kuneva, announced: "We need a root and branch review of consumer rules. At the moment, consumers are not getting a fair deal online, and complex rules are holding back the next generation of bright business ideas. We must find new solutions to new challenges. The question is can we afford to have 27 mini-online markets in Europe, denying consumers choice, opportunity and competitive prices? We need to inject a new sense of consumer confidence into the e-shopping world so it becomes a trusted market space. The rules of the game have changed, it's time for consumer policy to respond".

Although we have been living with European Union driven consumer law for some time now, the eight different sets of rules are complex and overlapping and have always been fraught with difficulty from a practical perspective.

For example, can the consumer open sealed packaging and still get a refund? Can the online retailer withhold some of the refund money paid if the returned goods arrive in a shoddy or used condition? What rights does an online retailer have to refuse a cancellation where self-assembly items have been partially assembled? Believe it or not, there have even been arguments about how soon a refund must arrive in the consumer's account based on the placement of a comma in the Distance Selling Regulations!

The E.U. Commission will, amongst other things, be considering key areas for online retail in the United Kingdom: clarifying rules applicable to cooling off periods; clarifying and simplifying the rules on how to return products; setting common rules on who pays the costs of returning products; simplifying which remedies are available to consumers; considering whether certain rights applicable to goods should be extended to services.

A copy of the press release can be found at *www.europa.eu/rapid/pressReleasesAction.do?reference=IP/07/158&format=HTML&aged=0&language=EN&guiLanguage=en*

According to Forrester Research, the market for online retail sales in Europe is set to more than double in under five years to reach 263 billion in 2011, with the number of shoppers growing to 174 million. With that many customers, if you are an online retailer, it pays to get involved in the consultation to help shape an online business environment that works for you.

