103:International Privacy Law

Paula Barrett
Partner
Eversheds LLP

Eugene M. FitzMaurice
former Counsel
Towers Perrin

Giuseppe Sanna
ACC Europe Secretary of the Board
Head of Advocacy

Faculty Biographies

Paula Barrett

Paula Barrett is a partner in Eversheds' information technology and e-commerce practice in the United Kingdom and leads the international data privacy group. Ms. Barrett's extensive experience in data protection/privacy law includes managing multi-jurisdictional compliance programs, advising on appropriate strategies for dealing with extra-EEA transfers of personal data, and the implementation of international data privacy policies. In her IT practice, she has in-depth experience in advising customers and suppliers on a wide range of IT contracts in both the public and private sectors. She has particular expertise in advising clients on outsourcings, strategic partnerships and major supply contracts, and e-commerce and technology regulation.

Prior to joining Eversheds, Ms. Barrett practiced in the media, computer, and communications group at Clifford Chance.

Ms. Barrett is a member of the Society for Computers and Law and the Data Protection Forum. She co-authored "EU Data Protection-A Compliance Guide for US Counsel" which appeared in the *ACC Docket.*

She attended Leeds Metropolitan University.

Eugene M. FitzMaurice

Eugene M. FitzMaurice is former counsel for Towers Perrin in Philadelphia.

Prior to working at Towers Perrin, he was with Adelphia Communications. Before then, Mr. FitzMaurice worked for ARCO's United States headquarters, where his corporate litigation experience involved environmental, product liability, and toxic tort claims. He also managed several M&A matters and had international responsibility for both corporate and litigation issues. The most protracted trial was a tri-partite suit brought simultaneously before the European Union, the Spanish Court for the Defense of Competition, and the International Arbitration Association in Paris. He also spent four years in England as European counsel, which included M&A, EU regulatory lobbying and compliance, and general corporate law.
After law school, he worked for Atlantic Richfield, where his work included trying cases on behalf of the refining and marketing division and representing ARCO as a lobbyist.

Mr. FitzMaurice graduated from Boston College Law School.

Giuseppe Sanna

Until recently Giuseppe Sanna was head group of legal at mmO2 plc based in London.

Previously he was general counsel Europe, Middle East, Africa, India for GE Consumer & Industrial. During his career Mr. Sanna has work in high tech, FMCG and telecommunication industries, mainly concentrating on corporate and antitrust related work.

He serves as ACCE's secretary of the board and head of advocacy. In this capacity, he has assisted on initiatives at EU level on legal privilege as well on liberalization of the legal profession. Mr. Sanna has extensively lectured in Europe and the U.S. in legal departments management, antitrust, and privacy law. He has also participated on school community projects and charitable events in the UK.

Mr. Sanna graduated with a MA in international relations from Johns Hopkins University, School of Advanced International Studies in Washington, DC. Mr. Sanna has trained at ENA in Paris and also studied law and political science in Italy.

Session 103
International Privacy Law

Guiseppe Sanna - ACCE

Paula Barrett - Eversheds

Gene FitzMaurice

Privacy Laws – A Global Phenomenon

Giuseppe Sanna
ACCE

Privacy Laws – Global Phenomenon

- EU Legal Framework
  - Data Protection Directive
  - Electronic Communications Privacy Directive
- All Member States other than France have implemented the EU Data Protection Directive
  - France has a pre-existing law and is in process of revising that law
- Growing number of laws around the world
  - *E.g.*, Argentina, Australia, Canada, Chile, Hong Kong, Israel, Japan, New Zealand

Assumptions and Caveats

- Many of you have substantial expertise concerning data privacy issues
- Privacy issues too numerous to cover comprehensively in available time
- Focus on selected issues – in particular, issues likely to be of interest to a substantial number of diverse companies

Special Concerns - Accession Countries

- All Accession Countries have implemented privacy laws/regulations based on the EU Data Protection Directive
- Most Accession Countries have not yet implemented the Electronic Communications Privacy Directive
- Same is true of nearly half of the pre-existing Member States
- Possible legal action by the Commission to force Member State implementation of the Electronic Communications Privacy Directive

ACC's 2004 Annual Meeting: The New Face of In-house Counsel October 25-27, Sheraton Chicago

Special Concerns - Accession Countries

- Extensive reform prior to accession
  - Raft of post-2000 legislation inspired by accession
  - Newly created data protection agencies
- Relatively untested data protection regimes
  - Many regimes not fully mature
  - Limited case law or other interpretive guidance
- Future changes likely
  - Most regimes apply EU rules but important differences remain
- Relatively untested data protection agencies
  - Some agencies lack independence/real enforcement authority – *e.g.*, Hungary (right of referral only)

ACC's 2004 Annual Meeting: The New Face of In-house Counsel October 25-27, Sheraton Chicago

Special Concerns - Accession Countries

- Variable on-ground enforcement of data protection laws/regulations in Accession Countries
  - Some national agencies engage in active enforcement
    - Poland (184 investigations in 2003); Czech Rep. (35 investigations in 2003)
  - Other agencies are less active
- Variable penalties for non-compliance
  - Penalties range from slight to serious – *e.g.*, over €600,000 in Czech Republic vs. approximately €3,000 in Estonia
  - Significant penalties still rare although gradually changing
- Enforcement focus on public bodies and certain private businesses
  - Privacy regulators concerned with misuse of personal data by public authorities and national data registries
  - Key private sectors under scrutiny – health; marketing/telemarketing; banking; insurance

ACC's 2004 Annual Meeting: The New Face of In-house Counsel October 25-27, Sheraton Chicago

Impact on Multinationals

ACC's 2004 Annual Meeting: The New Face of In-house Counsel October 25-27, Sheraton Chicago

The in-house bar association.℠

Impact on Multinationals Example – HR Data

- Privacy rules apply to personal information collected from or generated about employees
  - Payroll data
  - Work telephone number
  - Expense reimbursement data
- They restrict what can be done with the information
  - Monitoring of employees' computer use is strictly limited
  - Use of sensitive information, such as information about health, race, or religion, is restricted
- They give employees certain rights
  - Employees have a right to review evaluations
  - Employees and work councils must be informed of the information being collected, the purposes for which it is being used, and any transfers outside the EU
- Use of consent is problematic

ACC's 2004 Annual Meeting: The New Face of In-house Counsel October 25-27, Sheraton Chicago

Impact on Multinationals Example - Websites

- Only information related to declared purpose can be collected
- Invisible collection of information without notice is prohibited
- Stringent security requirements
- Consent needed for subsequent use of information for direct marketing
- Use of cookies is subject to additional requirements (disclosure/opt-out opportunity)

ACC's 2004 Annual Meeting: The New Face of In-house Counsel October 25-27, Sheraton Chicago

ACC Association of Corporate Counsel

Impact on Multinationals Example – Intra-Group Transfers

- Data often shared globally throughout companies – Examples include
  - Global address book
  - Consolidated HR and customer databases
- Transfers of personal data to third countries are restricted unless those countries offer "adequate" protection
- M&A issues: entities may not have compatible compliance strategies
- Companies in a corporate group often provide data processing services to other group members
  - These must be covered by a processing contract

ACC's 2004 Annual Meeting: The New Face of In-house Counsel October 25-27, Sheraton Chicago

ACC Association of Corporate Counsel

Why Should Multinationals Comply?

- Because it is a legal requirement
- To ensure good relationships with employees and customers
  - Non-compliance can lead to employee complaints, straining relations with works councils
  - Privacy protection is increasingly used as a competitive advantage in obtaining and retaining customers
- Liability
  - Potential civil and criminal sanctions for company and possibly individual officers
- Enforcement
  - Enforcement by Data Protection Agencies is increasing
  - Some can impose administrative fines
  - Some adopt a name-and-shame approach that may harm image and reputation

ACC's 2004 Annual Meeting: The New Face of In-house Counsel October 25-27, Sheraton Chicago

How Can Multinationals Comply?

- Conduct assessment of company's personal information practices
  - Who collects and processes what personal information?
  - For what purposes?
  - To whom is personal information disclosed and why?
  - What security measures are in place?
  - Are employees trained regarding privacy obligations?
  - Does the company provide notice of information practices?
  - Has the company made required regulatory notifications?
  - Does the company transfer data abroad and, if so, does it have mechanisms in place to ensure adequate protection?

How Can Multinationals Comply?

- Implement detailed internal policies for:
  - Data processing activities by department (*e.g.*, HR and IT)
  - Use of computers by employees and related monitoring
  - Security systems
- Establish clear lines of responsibility and appoint a chief privacy officer
  - Supplement with personnel knowledgeable about privacy in each business unit to field straightforward questions
- Execute privacy contracts with service providers
- Perform regular assessments to verify compliance and address possible deficiencies

Realities of Enforcement

- Increasingly pro-active approach
  - Italy – checking compliance with transfer rules
  - UK – reviewing web site compliance
  - France – "Operation Spam Box" targeting spammers
- Regional enforcement trends evident
  - Stricter – France, Italy, Spain, Germany
  - Softer – UK and Scandinavia
  - EE?
- Notable increase in complaints/cases:
  - UK – 91 criminal cases (2003)
  - Austria – 85 complaints/year
  - Spain – 541 investigations (2003)

Realities of Enforcement

- Significant sanctions currently rare
  - Spain – Microsoft fine (approx. $40,000)
  - Italy – fines up to €15,000
  - UK – fines up to € 5,000
- Reputational risk remains high
  - France – Nikon France v. M. Frederic (2002); employee monitoring violates French law

International Transfers

Paula Barrett
Eversheds

Transfers outside of EEA

- Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an *adequate level of protection* for the rights and freedoms of data subjects in relation to the processing of personal data

Transfer outside of EEA

- EEA? - EU (25 countries) and Iceland, Liechtenstein and Norway
- The EU Commission decides whether a country has adequate protection
- Currently (01/09/04)
  - Hungary
  - Switzerland
  - US companies signed up to "Safe harbor"
  - US-transfer of Air Passenger Name Record Data
  - Canada though not entirely
  - Argentina
  - Guernsey
  - Isle of Man

Transborder Transfer Mechanisms

- Does derogation apply?
  - Data subject consents (not all countries allow e.g. France)
  - Necessary to perform contract with data subject
  - Necessary for conclusion or performance of contract with third party concluded in interest of employee
  - Necessary for establishing, defending or exercising legal claims
  - Necessary to protect vital interests of the data subject

Consent

- Sensitive Data - must be explicit. Usually required in writing.
- Other Personal Data

  "… any freely given specific and informed indication of his wishes by which the data subject *signifies* his agreement to personal data relating to him being processed"
- Silence/no response is not consent
- Is employee really "free" to give consent?

Transborder Transfer Mechanisms cont.

- If exemption doesn't apply need to ensure adequacy
  - Self Assessment of Adequacy
  - US Safe Harbor Registration
  - EC Model Clause Contract
  - EC Approved Binding Intra Group Rules
- Pros and Cons to each of these
- Consider other practical steps e.g. can data be anonymised before transfer

Self Assessment

- No real guidance
- Risk assessment
- Time, expense and no guarantees
- If undertaken will need to take further steps
  - keep assessing
  - further precautions

Safe Harbor

- US only
- Not all sectors covered
- Annual audit and certification
- Potential for class actions
- Investigation and Fines from FTC
- Low take up

EC Model Contracts

- Processor and Controller to Controller versions
- but:
  - "Euro speak"
  - onerous e.g. joint & several liability and cross indemnities
  - may implement own version (e.g. as drafted by Eversheds) but less certain to achieve goal (though that is a low risk?)

Binding Corporate Rules

- New Solution - Only applicable for intra-group transfers
- The rules must
  - be binding internally & externally
  - be legally enforceable by data subjects & data protection authorities
  - contain a duty to inform the data protection authority if a member of the corporate group may be unable to fulfil its obligations, if this will have a substantial effect
- Individual Approval by Commission or Member State data protection authorities

ACC Association of Corporate Counsel

Other Concerns

- Fair Processing
  - still need to inform individual that transfer may take place and where to
  - still need legitimate reason to carry out processing
- Prior approval from local regulatory body may still be required in some jurisdictions
  - for transfer outside EEA e.g France
  - to process sensitive data e.g. Spain

ACC's 2004 Annual Meeting: The New Face of In-house Counsel October 25-27, Sheraton Chicago

The dean of the Harvard Law School said, in 1998, that by the end of the Twentieth Century, there would be more lawyers than people in the United States. The century has turned, and we are still a bit shy of that magical equation, but the proliferation of privacy laws, here and in other countries, almost guarantees that more and more young people, whether of a libertarian or litigious bent, will turn to the law.

Perhaps the most famous privacy statue is one of the most recent: HIPAA, or the Health Insurance Portability and Accountability Act of 1996. Corporations sometimes ask, "Who is covered by the Act?" and the answer is, "You are."

On a more limited basis, you are covered if you are an individual or group plan providing or paying for the cost of medical care. This includes heath and dental plans, prescription drug insurers, and HMO's, Medicare supplement insurers, Medicaid, and others. The implementation date was April 14, 2003 for all entities other than "Small Health Plans", whish are those with $5 million or less in annual receipts. The effective date for those plans was April 14 of this year.

Every heath care provider, regardless of size, is a covered entity if it transmits electronically such data as claims, benefit eligibility requirements inquiries, and referral authorization requests. Simply using e-mail does not make a health care provider a covered entity; the transmission must be in connection with a standard transaction.

A person, real or corporate (other than a member of a covered entity's workforce), that performs functions on behalf of a covered entity, where those functions include the use or disclosure of individually identifiable health information, is a business associate ("BA").

Services performed by a business associate must be under a Business Associate Contract. The covered entity's contract must impose specified written safeguards on the individually identifiable health information used or disclosed by the BA.

The Privacy Rule covers all "individually identifiable health information", which is held or transmitted by a covered entity or its business associate, in any form or media, electronic, printed or oral. This data is termed PHI, or Protected Health Information.

Space does not permit a full listing of all the rules and exceptions. However, there are a few required disclosures: to individuals (or their personal representatives) when they specifically request access to their data, or ask for an accounting of disclosures of the PHI; and, to the United States Department of Health and Humans Services ("HHS"), in connection with compliance investigations or similar actions. (HHS has established a civil rights office, and its website is www.hhs.gov/ocr/hipaa. A full listing of required and permitted disclosures, as well as exceptions, can be found at the Office of Civil Rights' site under various headings including "Government Access Guidance" and "Treatment, Payment [and] Health Care Operations Guidance".)

No regulation would be complete without exceptions. One of the most important is that PHI can be reformatted to become "De-identified PHI." This is material used to create

information not individually identifiable, and which can also be disclosed to a BA for such purpose.

As our participants from other countries know, we have both state and federal laws here, and the federal law always pre-empts any state statute in this field. Almost. HHS can work with the state statutes to prevent fraud, or if illicit drugs are involved, or if there is a compelling public health or safety issue.

HIPAA has its own security regulations. A covered entity must ensure the integrity of PHI using appropriate hardware and software, and is allowed to consider the costs of security measures. Some of the standards imposed by HIPAA are required and some are "addressable" If you consider a standard "addressable" and can reasonably apply it to your business, you must do so. If not, you must document why you cannot do so. Large health plans must comply with these regulations no late than April 20, 2005 and small plans ($5 million or less in annual receipts) have one additional year.

A self-insured plan must have a Privacy Officer. If a fully insured plan receives PHI, it too must designate a Privacy Officer. In other words, if you receive only enrollment and summary data, you do not need a Privacy Officer.

That person must create the Privacy Plan, and implement it. If a Plan Sponsor must designate a Privacy Officer, it must also name a Contact Person. This person receives complaints and provides information regarding the plan's notice or of privacy practices. The Contact Person must be identified in any correspondence denying access to PHI. (The Privacy Officer and Contact Person may be the same individual.)

The Privacy Plan should have an overview of HIPAA, identification of what is subject to HIPAA and the Privacy Plan; identify the Privacy Officer and Contact Person (and discuss their training requirements) as well as provide a complaint and review procedure, and investigation methods. Perhaps most importantly from the individual's perspective, there must be an anti-retaliation measure.

The penalties for civil misuse can be $100 per incident, up to $25,000 per person, per year, per standard. Criminal penalties can go as high as $250,000 and ten years in prison for obtaining PHI with intent to sell, transfer or use it for personal gain or malicious harm.

There are also wide ranging privacy requirements in Canada. The Canadian Parliament enacted by Royal Assent the Personal Information Protection and Electronic Documents Act ("PIPEDA") on April 13, 2000. This requires individual consent for the collection, use, and disclosure of personal information. The Act takes its outline from the Model Code for the Protection of Personal Information approved in 1996 by the Canadian Standards Association. PIPEDA complements the Federal Privacy Act, which places similar restrictions on government institutions.

An early conflict, or at least concern, was raised when the Canadian Medical Association requested distinct rules for certain health data and commercial issues, particularly where PIPEDA, like the Model Code, was intentionally vague, and the Privacy Commissioner has great discretion in interpreting PIPEDA.

In the leading case, the Commissioner took a narrow reading of certain private rights. In The Commissioner's Finding on the Prescribing Patterns of Doctors, the Privacy Commissioner said that, for Health Canada to sell information about the patient's date of birth, gender, drug numbers, insurance information and the doctor's name and I.D. number, did not violate the law as it was not the sale of personal information. The Commissioner found it to be more like "work product." To do otherwise, the Commissioner said, "would have the effect of precluding many kinds of legitimate consumer reporting."

At the same time, Canada has struggled with questions of personal information, particularly where it may be of interest in the health and research fields. When discussing the need for stringent privacy regulations in medical research, one commissioner, Roy Romanow, Q.C., said, "[H]ealth research –especially biomedical and scientific research – is an increasingly important component of Canada's knowledge economy, … [but the Commissioners understand that while] researchers would… prefer to have access to 'person oriented' health information [this should happen only] when there are sufficient safeguards in place …"

PIPEDA requires that "every organization" that "collects, uses or discloses" personal information "in the course of commercial activities" take steps to protect individual privacy. There are four basic concepts:

"Every organization" includes traditional businesses, e-commerce, physicians, pharmacies and pharmaceutical and device manufacturers.

It covers the "Collection Use and Disclosure" of personal information. Collection deals with obtaining any data about an identifiable individual. Use addresses "anytime data about an identifiable individual is accessed, manipulated, altered, deleted, or destroyed within the organization." Disclosure deals with transmission outside the organization. This could include transferring clinical data to another government, such as the U.S. Food and Drug Administration.

The Privacy Commissioner states that collection, use and disclosure are entirely separate. One can consent to participate in a trial, but that does not imply consent to sell the results of the tests.

PIPEDA does not apply to government organizations subject to the Federal Privacy Act.

An organization subject to PIPEDA must identify the purpose for which it collects, uses and discloses data, and must adhere to those purposes only.

Since January 1 of 2002, no commercial entity can disclose information for consideration in one province if the information was collected in another, without the subject's consent. After January 1 of this year, no entity may collect data about anyone without the person's consent. That consent must be meaningful and freely given, two concepts which are thoroughly reviewed in PIPEDA.

In a manner somewhat analogous to HIPAA, an organization subject to PIPEDA must have a privacy policy, stating the intent of its data collection, methods for securing consent, and limits on use and disclosure. There must be an individual comparable to HIPAA's Privacy Officer and Contact Person. Such an individual must be identified. Organizations must have easy to use complaint procedures for individual data subjects. The individual also can complain directly to the Privacy Commissioner, who has broad powers to enforce investigate the complaint. The Commissioner however, has stressed a preference for voluntary resolution. Finally, a person may go to federal court.

There are other privacy concerns than broad reaching statues like PIPEDA and HIPAA, of course. Many of these deal with the Internet and e-mail usage in the office.

In late 2002, an Angus Reid poll found that Canadian workers spent only two hours each week searching the Net. I suspect the number was much higher. Studies in the U.S. say about ten hours per week is spent, a number I also suspect is low.

Cases in Canada seem as interested in the content of the e-mails sent as the use of an employer's system. In CELU vs. Celanese, the employee was discharged for using internal e-mail to protest the failure of the company to address concerns raised by his daughter (and fellow employee).

It appears that employers are being left to determine policies. Much will depend on whether the employer is subject to federal or provincial legislation, or is private or public. Knopf, in the Comparative Labor Law and Policy Journal, suggests PIPEDA should be the guide in establishing the rules. Canadian arbitration decisions seem to favor a reasonableness approach in these matters.

There are many more cases in the U.S., which is expectable given the extent of litigation. There are cases that an employee could be discharged for using the Internet, even where the employer told him he could so. This is different from the Canadian finding that, even where the employer owns the e-mail system, there is no complete right of management review or interception. See, the 2001-2002 Labour Arbitration Yearbook, at 45.

Finally, a company in either country needs to set forth clear guidelines. Tell the employees what use can and cannot be made of the e-mail system and Internet. Establish a secure and consistent control system, such as cookies or user registration. Manage use to protect yourself from lawsuits. Control anonymous postings. Establish and maintain an e-commerce in-house legal practice

