

# Current Topics in Privacy and Data Protection ISACA

Rosemary Jay – Partner

# Topics

- Is there privacy protection in the media after John Terry?
- Collecting personal data online – the new Code from the Information Commissioner
- The use of Assessments –current consultation
- How will the power to impose fines be used?
- Proposed changes to the electoral roll
- Revised model contract for overseas transfer of personal data
- Changes to the ePrivacy Directive
- Review of the general data protection Directive

# Privacy after the John Terry ruling

- Case law has developed to protect personal privacy from media intrusion
- Court orders may restrict reporting of the fact an order has been made “super injunctions”
- The court refused to grant John Terry an order restricting publication of allegations about his private life on grounds specific to the case
- The court did not have sufficient evidence to be satisfied that an order was justified
- It held that Terry was protecting his reputation and the commercial value of his name rather than his personal privacy

# Collecting personal data online – new Code consultation

- Draft code issued with consultation finishing on the 5 March
- Covers
  - Data protection on line
  - Collecting information from vulnerable people
  - Marketing goods and services on line
  - Privacy choices (including the use of cookies)
  - Operating internationally and cloud computing
  - Individuals' rights online

# Comments

- There is confusion about the scope of the Code and the level of identifiable information which is covered, which is compounded by the advice on subject access;
- Some useful material on publically available information (not “fair game”), the use of “off the peg” forms for data collection, behavioural advertising;
- Encourages on line providers to be clear about who “owns” which data and what privacy choices are available to users;
- On cloud computing advises that this can be acceptable subject to proper security guarantees.

# Assessments

- New power introduced by the Coroners and Justice Act 2009 to carry out “compulsory audits” of government departments, designated public authorities or designated persons;
- ICO serves an assessment notice to set out the powers he wishes to exercise which can include interviewing individuals, seeing paper, entering premises;
- Recipient may appeal against the notice;
- ICO must issue a code of practice setting out how the power will be exercised;
- Draft currently out for consultation.

# The use of Assessments by the Commissioner

- “the scope of our extended powers is at the moment relatively modest; as they only apply to government departments. However moving forward it is entirely reasonable to expect that, where the evidence supports it, I will seek to extend my powers to undertake compulsory audits in both the public and private sectors”
- Christopher Graham – Foreword to the consultation
- The power can be extended by secondary legislation

# What will happen after 6 April?

- ICO will be able to impose monetary penalties of up to £500,000.000 where
  - There has been a serious contravention of the Principles of the DPA
  - Likely to cause substantial damage or distress and
  - It was deliberate or reckless

The ICO must give notice of intent to serve such a notice and there is an appeal to the Tribunal against the notice or the amount of the penalty

Penalties will not apply to contraventions found when carrying out assessments

# Monetary Penalty Notices

- The notices must set out :
  - the nature of the personal data involved in the contravention;
  - the circumstances in which it occurred
  - The reason the ICO considers it is serious
  - The reason the ICO thinks it will cause substantial damage or distress
  - The nature of whether it was deliberate or reckless
  - The proposed amount of the penalty
  - When it is proposed to be served

# Guidance from the ICO

- Examples
- Serious contravention – the loss of unencrypted sensitive personal data
- Substantial damage – loss of employment
- Substantial distress- upset at loss of medical records
- Reckless – the controller has been warned of the risk and ignored it
- Will consider
  - Numbers affected, duration and extent, type of personal data involved, compliance and governance arrangements

# Will the electoral roll disappear?

- Current consultation on the possibility of withdrawing the edited electoral roll from use
- The full roll will still be available for money laundering and credit checks
- Will impact on the marketing industry and anyone who buys in mailing lists

# Revised model contract – does it help?

- There are 2 model contracts for transfers of data outside the EEA – controller to controller and controller to processor
- Many processors outside the EEA use sub-contractors to assist with processing
- The revised model allows for the use of sub-contractors
  - Consent of the controller is required
  - A written agreement between the processor and sub-processor which imposes the same obligations on the sub processor
  - Rights of data subjects and rights for the controller against the sub-processor to be included

# All change with ePrivacy

- The new rules must be in force in Member States from July 2011;
- Providers of public electronic services will have to notify regulators and subscribers of any serious security breaches;
- The storage of information or gaining access to information on the “terminal equipment of a user or subscriber” is only allowed on condition that the person has given consent having been provided with clear information, other than where the “cookie” is necessary for carrying out a communication or necessary to provide a service which has been requested

# Looking ahead – will the general Directive be altered?

- Commission launched a consultation on the Directive in July 2009
- The challenges facing the Directive are:
  - The incorporation of the Third Pillar areas post Lisbon;
  - The difficulties in dealing with the transfer of data outside the EEA
  - The challenges of globalisation
  - The differences in implementation across the EU

# Looking ahead to changes

- Global standards
- Internationalisation
- New mechanisms for transfer of data
- Dealing with policing and security data
  
- UK data sharing initiatives
- Privacy by Design
- PIAs
- Increased powers of regulators

**QUESTIONS?**

*Working hard to make it easier*



Pinsent Masons

**Rosemary.Jay@pinsentmasons.com**

0161 234 8734

*Working hard to make it easier*



Pinsent Masons

# *Working hard to make it easier*

LONDON DUBAI BEIJING SHANGHAI HONG KONG SINGAPORE  
OTHER UK LOCATIONS: BIRMINGHAM BRISTOL EDINBURGH GLASGOW LEEDS MANCHESTER

Pinsent Masons LLP is a limited liability partnership registered in England & Wales (registered number: OC333653) and regulated by the Solicitors Regulation Authority. The word 'partner', used in relation to the LLP, refers to a member of the LLP or an employee or consultant of the LLP or any affiliated firm who is a lawyer with equivalent standing and qualifications. A list of the members of the LLP, and of those non-members who are designated as partners, is displayed at the LLP's registered office: CityPoint, One Ropemaker Street, London, EC2Y 9AH, United Kingdom.

We use 'Pinsent Masons' to refer to Pinsent Masons LLP and affiliated entities that practise under the name 'Pinsent Masons' or a name that incorporates those words. Reference to 'Pinsent Masons' is to Pinsent Masons LLP and/or one or more of those affiliated entities as the context requires. For important regulatory information please visit: [www.pinsentmasons.com](http://www.pinsentmasons.com).

© Pinsent Masons LLP 2008



Pinsent Masons

[www.pinsentmasons.com](http://www.pinsentmasons.com)