

Identity & the Law

Dr Ian Walden
Consultant, Baker & McKenzie
CCLS, Queen Mary, University of London

Introduction

- Signatures
 - validity, enforceability & admissibility
- Personal data
 - Data Protection Act 1998
 - confidentiality
- Identity theft
 - criminal law



Signatures

- Legal requirements/practice
 - e.g. Consumer Credit Act 1974
- Legal definitions
 - copies & equivalents
 - "signature" includes a facsimile of a signature by whatever process reproduced"
 - personal signatures, e.g. *In Re a debtor* [1996] 2 All ER 345
- Signature functions
 - identity, e.g. *Goodman v J.Eban Ltd* [1954] 1 All ER 763
 - intention to be bound
 - validate integrity of document
 - person to signature, signature to document

International Developments

- United States
 - Uniform Electronic Transactions Act 1998
 - s.9(a) "An electronic record or electronic signature is attributable to a person if it was the act of the person. The act of the person may be shown in any manner, including a showing of the efficacy of any security procedure applied to determine the person to which the electronic record or electronic signature was attributable."
 - Electronic Signatures in Global and National Commerce Act 2000
 - 15 USC § 7001: "a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form"
- UNCITRAL Model law on Electronic Commerce (1996)
 - Article 7(1)(b) "that method is as reliable as was appropriate for the purposes for which the data message was generated..."
- Model Law on Electronic Signatures (2001)

Directive 99/93/EC

- Definitions (art. 2)
 - 'advanced electronic signature'
 - "it is uniquely linked to the signatory;
 - it is capable of identifying the signatory;
 - it is created using means that the signatory can maintain under his sole control; and
 - it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable"
- Legal effects (art. 5)
 - 'satisfy' and 'admissible'
 - advanced electronic signature; with qualified certificate and created by a secure-signature-creation-device
 - 'not denied legal effectiveness'

UK Law

- Electronic Communications Act 2000
 - s. 7 re: admissibility
 - s. 8. secondary legislation
 - e.g. The Companies Act 1985 (Electronic Communications) Order 2000 (No. 3373)
- The Electronic Signature Regulations 2002 (SI No. 318)
 - 'advanced electronic signature'
 - re: certification service providers

Personal Data

- 'identifiable directly or indirectly'
- fair and lawful processing
 - limited right to object
 - direct marketing, substantial damage or distress
- one or more specified purposes
 - data sharing
- offence of unlawful obtaining (s. 55)

Confidentiality

- Equitable action for breach of confidence
 - quality of confidence, obligation of confidence and unauthorised use
 - *R v Department of Health, ex parte Source Informatics* (2000) 1 All ER 786
 - *A v B and anor sub nom Gary Flitcroft v Mirror Group Newspapers Ltd* (2002) 2 All ER 545
 - no need for a new cause of action

Identity Theft I

- Cabinet Office Report (July 2002)
 - Interdepartmental Identity Fraud Forum (IIFF)
 - current inadequate response
 - gov. departments lack prosecution arm
 - low priority given to area
 - lack of specific offence
- Entitlement Card Consultation Paper
 - offence to “use a means of identification of another person or a fictitious person without reasonable cause”
 - summary only, max. 6 imprisonment
 - defences

Identity Theft II

- *Oxford v Moss* (1979) 68 Cr.App.R. 183
- Computer Misuse Act 1990
 - unauthorised access & modification
- Fraud
 - obtaining property/services by deception
 - e.g. *R v Moritz* (1981)
 - e.g. Passport application fee: £28
- Forgery and Counterfeiting Act 1981
 - e.g. *R v Gold* [1988] AC 1063

Identity Theft: US Law

- Identity Theft and Assumption Deterrence Act of 1998 (18 U.S.C 1028)
 - "Knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid and abet, any unlawful activity..."
 - e.g. 'unique biometric data', 'address or routing code'
 - from 15 - 25 years imprisonment
 - illegal under the laws of 49 States
- Federal Trade Commission
 - centralised reporting and consumer education facility



Concluding Remarks