

Managing the Data Explosion

Francis Aldhouse

NCC Annual Conference: Sustainable IT. 10th & 11th June 2008



What Data Explosion?

- ▼ More pervasive technologies & more intensive data use
 - ▼ Behavioural profiling of web-site users
 - ▼ Social networking
- ▼ Public service data sharing
- ▼ Enhanced law-enforcement access to data
- ▼ Customer service at a distance
- ▼ Commercial and public sector drivers
- ▼ Technology enablers
- ▼ Potential for greater harm to individuals
- ▼ Enhanced risk: Avoidance? Mitigation? Safeguards?



Events, dear boy. Events.



What events?

- ▼ HMRC – 2 CD-Roms with data on 25 million individuals sent to NAO and lost in the post – revealed Nov 2007
 - ▼ Feb 08 phishing attack offering victims £210 tax rebate
- ▼ Driving Theory Test candidates – 3 m UK records on hard drive lost by Pearson in Iowa – Dec 2007
- ▼ Ministry of Justice CD's lost in post 15 Dec 2007
Manchester Magistrates' Court defendants



More of the sorry tale

- ▼ 600,000 armed forces applicants' data for the last ten years were stolen with an MoD laptop in January 2008
 - ▼ includes names and addresses, passport details, national insurance and NHS numbers
- ▼ A laptop containing medical records for more than 5,000 people stolen from Russells Hall Hospital near Dudley on 8 Jan 2008
- ▼ Nothing new – in 2001, 1354 government computers lost or stolen



Not just the Public Sector

- ▼ Monster.com job search website –
 - ▼ 1.6 million – mostly US - records stolen by a trojan in August 2007
- ▼ 45.6 million credit/debit card records stolen in US from TJ X – TK Maxx in the UK - between 2005 and 2007
- ▼ UK Retail Banks leaving personal information in unsecured refuse – Undertakings given to ICO in February 2007



Nationwide BS & Norwich Union

- ▼ Commissioner's big brother – Financial Services Authority
- ▼ **Nationwide** - Employee's laptop stolen from home; confidential data; 3 week delay
- ▼ Breached Principle 3 of the FSA's Principles for Business
- ▼ Penalty: £ 980,000
- ▼ **Norwich Union Life** - Fraudsters used publicly available information to have customer records altered and policies fraudulently surrendered
- ▼ Fined £1.26m – 10 December 2007 – 30% discount
- ▼ Breach of FSA Principle 3
- ▼ **Inadequate assessment of risk of financial crime and failure to protect customers**



Is this a problem?

- ▼ Identity Theft 258,427 32% of complaints in 2007
 - ▼ US FTC *Consumer Fraud and Identity Theft Complaint Data*
- ▼ Wild West Internet – 76 arrested in Spain on 10 Feb 08 for €3bn E-Bay auction fraud
- ▼ Six out of ten UK citizens do not believe their data is safe with government departments - Ipsos/MORI 28 and 29 November 2007 sponsored by Symantec
- ▼ Corrosive environment destroying trust
- ▼ Imposes extra transaction costs
- ▼ Does it tell the truth about how government and business 'respect' UK citizens and customers?



A legal problem

- ▼ S. 4 (2) Data Protection 1998 imposes duties on data controllers to process personal data fairly, lawfully, in accordance with the rest of the 8 Principles.
- ▼ Principle 7
- ▼ Technical & organisational measures to be taken against
 - ▼ Unauthorised processing
 - ▼ Unlawful processing
 - ▼ Accidental loss
 - ▼ Accidental destruction, or
 - ▼ Accidental damage



When things go wrong - Enforcement

- ▼ The Regulator - UK Information Commissioner
- ▼ Enforcement Notice against data controller for breach of Principle – order to remedy breaches
 - ▼ Undertakings – February 2007 Retail Banks: lost customer data
 - ▼ ISO/IEC 27000 series – especially 27002 successor to BS 7799
 - ▼ Laptop encryption
- ▼ Unlimited fine
- ▼ Personal liability of directors and officers
- ▼ Community service



New sanctions

- ▼ Commissioner's big brothers – e. g. Financial Services Authority
 - ▼ Nationwide Building Society
 - ▼ Norwich Union
- ▼ Ss 77 & 144 Criminal Justice and Immigration Act 2008 - if brought into force
 - ▼ Commissioner's new powers to impose administrative fines
 - ▼ Two years imprisonment for blagging



A Policy Problem

- ▼ 'Costliness' of mistrust
- ▼ Dubious statistics:
 - ▼ Eurobarometer 2008: 73% support internet monitoring to fight terrorism
- ▼ How to create real trust
- ▼ Efficient Data Protection
 - ▼ The necessary conditions to create a context in which individuals can go about their normal lives with informed confidence



Two Policy Objectives

- ▼ Alignment of business motivation and individual interests – make it natural to deliver good outcomes
- ▼ Government culture change – data protection must be taken seriously and not treated as an inconvenience
 - ▼ Modernising Government White Paper March 1999 – ‘our belief that data protection is an objective of information age government, not an obstacle to it.’
 - ▼ Transformational Government Strategy paper of Nov 2005 – ‘a balance between maintaining the privacy of the individual and delivering more efficient, higher quality services with minimal bureaucracy.’



Events, dear boy. Events.



How has the Government reacted?

- ▼ Information Commissioner Richard Thomas will be given the power to "spot check" departments and examine the quality of compliance. Gordon Brown PMQs 21 Nov 2007
- ▼ Cabinet Office Report – December 2007
 - ▼ Data Handling Procedures in Government: Interim Progress Report
 - ▼ Departmental reviews carried out
 - ▼ Governance work and recommendations
 - ▼ Annual Report
 - ▼ Statements of Internal Control
 - ▼ Notification of incidents
 - ▼ ICO powers of audit in whole public sector
 - ▼ New DPA sanctions
 - ▼ Further report Spring 2008 ?
- ▼ New statutory sanctions



What is to be done?

- ▼ Government and private sector
- ▼ New sanctions as an indicator and motivator
- ▼ Public and Private sectors:
 - ▼ Tougher internal procedures?
 - ▼ A change of heart and culture?
- ▼ Planning in Advance – or Privacy Impact Assessments
- ▼ A Culture of Privacy – compare OECD's Culture of Security



Other issues to watch

- ▼ Breach Notification
 - ▼ US model – California SB1386 in 2003 – now 42 states
 - ▼ European Union Electronic Communications proposal
- ▼ House of Lords Science and Technology Committee 24 July 2007 - the threat to the internet posed by e-crime
 - ▼ Call for Data Breach Notification law, and more: enhanced enforcement, British Standards, bank liability for security breaches
- ▼ House of Lords Constitution Committee on-going Surveillance Enquiry
- ▼ European Commission review of Framework Directive 95/46/EC in 2010



Au revoir

