



The “Regulatory Bear Market” The new legal environment for data security

Stewart Room

Partner, Privacy and Information Law Group

stewart.room@ffw.com

+44 (0) 207 861 4850

November 2009

Hypothesis

- Research for new book “Data Security Law and Practice” (www.lexisnexis.co.uk) has resulted in conclusion that a “Regulatory Bear Market” for data security is being built.
- Clear evidence for this is provided by the US and UK examples.
- Evidence is appearing at EU level too.
- There are clear actions for data controllers and processors.



What is a regulatory bear market?

- Not intended to be a pejorative statement.
- Compare with a financial bear market = negative sentiment and loss of confidence
- These factors are present in a regulatory bear market:
 1. About the ability/willingness of organisations to comply with the law
 2. About the law's ability to bring organisations in to compliance
 3. About the regulators own ability to achieve their objectives



Other features within a regulatory bear market

- A process of law reform
- New rules for best practice
- A willingness to be more prescriptive
- Tougher regulatory responses and increased regulatory activism
- Heightened focus on transparency and penalties
- More disputes and litigation



The US example – breach notification

- 2003 – California starts the process
- Greater transparency
- Focus on encryption
- Power shift from regulated to regulator and individuals affected
- Mitigation – “early warning system”
- Consequences include more disputes and litigation

The UK example

- 2006 – Information Commissioner starts campaign for new powers and penalties (“What price privacy?”)
- 2007 – Tougher regulatory responses (inc. FSA fines Nationwide £980,000)
- Nov 2007 – HMRC data loss affecting 25,000,000 UK citizens
- Nov 2007 – “Our approach to encryption”
- Dec 2007 – “The case for amending the Data Protection Act”
- March 2008 - Breach notification guidance
- May 2008 – Criminal Justice & Immigration Act (financial penalties)
- June 2008 – “Data Handling Review”
- Jan 2009 – Coroners & Justice Bill
- July 2009 – FSA fines HSBC +£3,000,000
- Sept 2009 – Conservatives’ proposals

Regulatory bear market at EU level (1)

- Nov 2007 – European Commission proposal to amend security provisions in Dir 2002/58/EC, to introduce breach notification obligation for providers of publicly available electronic communications services
- Sep 2008 – European Parliament expands obligation to anyone with an internet presence
- May 2008 – European Parliament Resolution understood to be compromise position



Regulatory bear market at EU level (2)

- NRA audit power
- NRA to issue recommendations on best practice
- Notify NRA of “personal data breach” “without undue delay”
- Notification to subscribers/individuals affected if (a) not implemented encryption or (b) NRA orders this
- Contents of notification
- Inventory of breaches

Regulatory bear market at EU level (3)

- 23 October 2009 - Commissioner Reding's speech on breach notification:

“The Telecoms Reform has put the issue of mandatory notification of personal data breaches firmly on the European policy agenda. The reformed telecoms package, now awaiting final agreement, will establish rules concerning the prevention, management and reporting of data breaches in the electronic communications sector. As you are aware, the Commission will go a step further to extend the debate to generally applicable breach notification requirements and work on possible legislative solutions.”



Actions

1. Establish Information Security Committee
2. Establish Incident Response Team
3. Review legal obligations relating to your data
4. Review your security policy, dovetailing with ISO 27000 and other standards for best practice
5. Review your project initiation rules
6. Review your rules for use of processors and sub-contractors
7. Review your rules for worker monitoring
8. Review your IT security
9. Implement necessary changes
10. Train on those changes