Field Fisher Waterhouse

Cybersecurity legal overview

Commonwealth Cybersecurity Forum 2014

Stewart Room
Partner, Privacy and Information Law Group
Director, Cyber Security Challenge UK
President, National Association of Data Protection Officers
6th March 2014

The nut and bolt has innumerable uses in countless industries, providing fundamental structure and strength. It's amazing how just one simple connection can be the basis for a successful relationship.

- The pillars of cybersecurity law and current reforms.
- Connecting cybersecurity and the common law.
- Regulatory agendas and right outcomes.

Pillars of Security Law | © Stewart Room | Twitter @StewartRoom		
General Privacy	E-Privacy	Cyber
Security of Personal Data	Security of Communications Networks & Services over which Personal Data are carried	Security of Critical Infrastructure
DP Directive 1995	PEC Directive 2002; Citizens Rights Directive 2009	PEC Directive 2002; Better Regulation Directive 2009
Controllers	Telcos; ISPs	Telcos; ISPs
Appropriate T&O measures	Approp. T&O; Breach Disclosure; Regulatory Audit	Approp. T&O; Breach Disclosure; Regulatory Audit
Draft GDP Regulation 2012	No change	Draft NIS Directive 2013; Draft PS2 Directive 2013
Controllers; Processors	No change	Markets Operators; Public Authorities; Payment Services Providers
Approp. T&O; Breach Disclosure; Regulatory Audit	No change	Approp. T&O; Breach Disclosure; Regulatory Audit

- Cybersecurity and data protection legislation coalesce around a need for entities to take “appropriate technical and organisational measures” for security and to be transparent about failures.
- The duty of care in tort is established where parties are sufficiently proximate to one another, it is reasonably foreseeable that harm may be suffered by their acts or omissions and it is reasonable to impose a duty of care (compensation is awarded for loss and damage that is not too remote).
- Where a duty of care is established, there is a duty to take “reasonable care”.
- There is a close similarity between the idea of reasonable care and appropriate technical and organisational measures.
- The detailed requirements of the duty are described by experts.

Regulatory agenda and outcomes

- Cybersecurity legislation seeks to incentivise compliance through the application of sanctions and penalties (stick, not carrot).
- Breach disclosure is a transparency mechanism that aids mitigation of harms and prevention of incidents.
- But breach disclosure to regulators creates a sausage machine of entities notifying breaches of law that lead to application of sanctions and penalties.
- Query whether these regulatory agendas create a negative incentive for entities?