Federated Identities, 'Circles of Trust' & Decentred Regulation in M-Commerce

ESRC E-Society Programme

The UK Data Protection Act 1998 has been in force for some years and is based on a European Directive that was initially proposed some 15 years ago. In that time, both the technological environment and commercial business models have changed out of all recognition, notably in the areas of electronic commerce (e-commerce) and mobile communications (m-commerce), leading to questions about the Act's continuing viability as the basis for an appropriate regulatory model for data protection in the Information Society. Andrew Charlesworth from the University of Bristol investigated the data privacy implications of new models of m-commerce, from the viewpoint of regulators and those regulated, to assess the future dynamics of data privacy regulation.

- The size and resourcing of EU Member State National Information Commissioners (NICs) plays a key role in their regulatory strategies.
- NICS in long-standing Member States with developed digital markets were more familiar with issues arising from disaggregated data environments (DDEs), primarily the internet, and were more likely to have dealt with citizen complaints relating to them.
- Most NICS felt that the EU data privacy regulatory framework provided sufficient discretion in the use of regulatory mechanism, but there were divisions as to how such discretion should be exercised.
- There is an acknowledgement by the regulatees that simply ensuring formal compliance with current regulatory requirements will be an insufficiently flexible method of meeting public expectations and that more effective solutions may not be perceived as compliant regulators and regulatees.
- The project identified a number of overlapping regulatory mechanisms largely derived from existing regulatory practices in the EU.

Background

The widespread adoption of innovative new technologies for the purchasing of goods and delivery of services in key areas of commercial and government practice will, argue the researchers, inevitably undermine principal components of the current data protection regime. The range of technical innovations placing strain on the regimes includes:

- The advent of genetic testing and the ethical problems arising from the collection, use and disclosure of genetic data;
- The spread of CCTV surveillance systems and the fragmentation of surveillance ownership;
- The development of on-line disaggregated or dispersed data-sets, and their distributed nature.

Current situation suggests that while the present data protection regime may be just about acceptable to commercial operators in terms of provision of legal certainty, minimal disruption to commercial practices, and relatively low costs of compliance and/or enforcement, it currently runs a serious risk of future impotence in the face of ongoing shifts in technological and societal practices online. Without an equivalent shift in thinking about the nature of a future regulatory framework for data protection, the authors argue that we might find ourselves with a data protection regime under which:

- Data controllers in complex technological business environments are unable to, and increasingly unwilling to attempt to, match their business practices with regulatory requirements;
- Data subjects in complex technological business environments find their data protection rights rendered largely ineffective;
- Any chance of the long-promised development of a thriving market in privacy enhancing products and services will be snuffed out.

The Project

The focus of the research was on whether it was possible to develop a model data privacy regulatory instrument or instruments within the existing EU legislative framework which could address both the broad goals expressed by the regulators, e.g. the EU NICS, and the practical requirements of public and private sector organisations wishing to engage in m-commerce.

- Through semi-structured interviews and focus groups, the research explored a number of stages which investigated the following questions:
- Can the existing EU data privacy regulatory framework effectively and efficiently address realistic risks to data subjects in proposed models of m-commerce, or are new 'decentred' strategies more appropriate?
- What variables influence the NICS perceptions of the purpose, operation and effectiveness of data privacy regulation, and of their own role within it, and will 'decentred' regulatory strategies clash with these perceptions?
- How do 'regulatory-oriented conversations' inside and between FIM service providers impact on the general 'regulatory conversation' between regulators and regulated?
- Will 'decentred' regulation of data privacy risk effective regulatory capture by industry and would this always be necessarily be undesirable?

Implications of the research

The project identified a number of overlapping regulatory mechanisms, largely derived from existing regulatory practices in the EU, which, taken as a whole, provided the basis for a proposed regulatory framework for structured disaggregated data environments (sDDE), and also suggested possible elements that could support regulation of unstructured disaggregated data environments (uDDE). The regulatory framework is co-regulatory in nature, aiming to draw upon the interest of regulatees in ensuring trust in their processes amongst the public. In brief, for a structured DDE, the framework would consist of:

- A regulatory licensing process - prior to operating a structured DDE a licence would have to be obtained from the regulator. Licensing would require the production of a technical overview of the DDE, identification of classes of user, and demonstration of adequate inter-user agreements with regard to data privacy. Failure to adhere to good practice would result in revocation of the licence by the regulator.

- A form of binding contractual agreement between parties to the DDE - similar in nature to the binding corporate agreement between elements of the same corporate entity e.g. that adopted by GE and approved by the UK NIC but between independent corporate entities, or government departments.

- An independent agent - 'Personal Data Guardian (PDG)' - embedded in the structured DDE system to ensure compliance of parties to the DDE with the licence, and the binding contractual agreement, (with the power via the binding contractual agreement) to take action against parties that breach their DP obligations, and with reporting duties to the regulator, including the obligation to reveal breaches.

The PDG would include data subject representatives to reduce regulatory capture risks, and materials used in support of the licensing process would be made publicly available.

- The minimum standard of DP protection would be the DP Directive baseline, but structured DDEs would be able to offer a higher standard, perhaps as a means of competitive advantage. Where a higher standard was offered, the PDG and regulator would hold parties liable for performance to that standard (as with the position taken by the FTC in the US).

The aims of the framework are that adequate information about the operation of the structured DDE is made available to the public and to the regulator. The PDG oversees members of the DDE, interacts with public and regulator, and is subject to regulator audit. Breach of binding rules by parties to the DDE is subject to initial internal sanction by the PDG which reports to the regulator. Failure of the PDG to carry out its functions appropriately would result in regulator sanctions, including possible loss of licence.

Policy Lessons and Future Research

The project has demonstrated that the regulatory strategies pursued by EU NICs are influenced by their relationship with national governments, their perceptions of their own role and degree of influence, their staffing composition and size, and their desire/ability to be proactive to the implications of new technologies, rather than reactive. Equally, the effectiveness of those strategies depends upon the extent to which those regulated can see the value of organisationally internalising business practices which support those regulatory goals, so that compliance is more than a matter of simply meeting the letter of privacy legislation something which the research suggests is often

removed from the practical protection of data privacy.

The research has identified a number of future research priorities:

- The project could be extended to examine NIC practices outside the EU, for example in Canada and Australia, and comparing the effectiveness of those practices to the largely self-regulating US regime. Such an approach would include assessing how multinational companies adopt internal data privacy strategies to cope with the different regimes.

- There is scope to investigate the personal data guardian model further as a compliance tool, through the medium of developing corporate FIM networks, or through proposed government data sharing projects.

- Future research needs to address regulatory mechanisms for personal data use in super-scale unstructured DDEs.

Further Information

For more information on the research project, please contact:

Andrew Charlesworth
The Law School
Unviersity of Bristol
Wills Memorial Building
Queens Road
Bristol
BS8 1RJ

Email: a.j.charlesworth@bristol.ac.uk

The e-Society Programme

Funded by the Economic and Social Research Council and co-ordinated by the Department of Sociology at the University of York, the e-Society is a multidisciplinary programme of research that seeks to investigate how institutions, practices and behaviours are being changed by the technologies that constitute the digital age. This £5 million programme draws on the expertise of leading academics from across the UK. Launched in October 2003, the programme will run until the end of October 2007.

Further details of the projects in the programme can be found at Http://www.york.ac.uk/res/e-society/