

The politics of Information Governance

Slide 1

EURIM and The Politics of Information Governance

Philip Virgo, Secretary General

EURIM, www.eurim.org.uk

Slide 2

The Politics of Information Governance

The Political Triangle:

Access, Protection and Retention

What is EURIM

Current and Planned Legislation

National, EU, International

The Corporate Balancing Act

Practical Risk Assessment

Protection as a Service

Fight Your Corner for

RELEVANT REGULATION

Good evening. Thanks to the loss of a couple of CDs in the post, you have a window of opportunity for influence that will not come again. But you have, at best, only a couple of months to set the agenda. Then government and its regulators and tame consultants will fill the thought vacuum and suffocate what is left of our businesses with yet more overheads that will be equally irrelevant to what those to date have failed to prevent.

You have a unique opportunity. Use your voice now - before it is too late.

Slide 3

EURIM

The All-Party Parliamentary – Industry Group concerned with the politics of the Information Society

71 MPs, 16 MEPs, 26 Peers: inc. 9 Ministers (2 in cabinet),

+ committee chairs/presidents, ex-ministers, opposition spokesmen etc

31 Corporate Members

18 Associate Members (not for profits and small firms)

Observers from Cabinet Office, DCMS, DTI, Home Office, EU Commission, Ofcom, OIC etc. etc.

Funded by Corporate and Associate Members

The odd name is because EURIM was originally created to improve UK inputs to EU policy. It has since developed into a unique forum for politicians, officials, users and suppliers to work together on issues that are not already well addressed elsewhere.

That is usually because the issues cut across departmental, interest group or

professional boundaries and there is no consensus as to what should be done by whom.

Current Priorities

- Confidence in the On-line World
- Transforming Public Services Delivery
- Secure Information and ID Sharing

**Information Governance cuts across ALL
Current structures are part of the problem**

Society is now critically dependent on on-line systems. Confidence in their resilience and security is essential. The Internet may be resilient in theory but we access it over communications networks that have more bottlenecks than a brewery. Confidence that it is fit for purpose is not helped by the rising tide of spam and the near impossibility of reporting problems to anyone who will help or take effective action.

That is why we have been working for around 18 months to help produce a way forward that harnesses the leadership and competencies of the Industry to a non-bureaucratic partnership with Government, Civil Society and Parliamentarians across organisational and political boundaries. Many of you will be aware of the twin-track consultation in the run-up to the Internet Governance Forum in Rio organised by Alun Michael MP who leads the EURIM group on e-Crime.

Essentially his approach has been to create a UK IGF which will demonstrate, through UK leadership, that it is possible to have a coherent approach to Internet governance without creating a United Nations Agency, as some other Countries wish. At the same time he has identified the need to deal differently with on-line crime, whatever name or definition we use.

A suspicious public is unlikely to be willing to "leave it to Industry" or to "trust self-regulation" but traditional forms of public accountability mean that calling for

Government to take a lead will inevitably create regulation and bureaucracy. We therefore need a new approach to that allows an industry lead and builds on the many good approaches that already exist rather than duplicating or undermining them.

That is a very brief summary of an approach that you will hear much more about as the UK IGF is rolled out and as work develops to develop the UK Internet Complaints Centre. I very much hope that ISSA UK will be amongst the foremost supporters and that you can also interest some of the other chapters in support when the time comes to line up international co-operation.

For the avoidance of doubt I should stress that this approach is entirely complementary to the ACPO/Met plan for a Central eCrime Unit and to the Fraud Initiative that is now on the starting blocks. A joined up approach at the design stage may come as a surprise, but it seems to me an achievement that is well worth celebrating later this evening when we get to the drinks!

Meanwhile big centralised public sector systems are more vulnerable than most and the realistic use of technology to help deliver better-targeted public services at lower cost is EURIM's second priority.

And credible and practical processes for secure information sharing, linked to identity management are essential if we are to have any confidence in the on-line world, whether public or private sector.

Information governance cuts across all three of EURIM's priorities.

The UK's current fragmented, duplicated, convoluted and semi-incompatible regulatory regimes detract from, rather than support good practice. They also,

manifestly, fail to protect our businesses and customers from malpractice and recklessness.

The failure of the FSA to actively monitor Northern Rock, when its business practices moved way out of line in a market that was already known to be out on a limb, is a case in point

Summary of UK Data Retention Requirements

Perhaps the most irrational area of regulation is the Bermuda triangle of data access, protection and retention. I acquired this slide a few years ago from a speaker at a meeting on disaster recovery. The statutory and regulatory requirements to retain data range from days to decades. There are bans on sharing information unless expressly permitted and bans on keeping it longer than needed for business purposes balanced by requirements to keep for no other reason than that regulators or law enforcement might wish to see it as some future date. And, as the recent revelations from HMRC, DWP and the Ministry of Justice indicate, the supply of data for audit or regulatory purposes is a major point of vulnerability.

There was and is more on the way.

More Laws

Most is equally muddled and unfit for purpose – some is will actually make things worse, such as Basel II which will serve to divert attention from liquidity, the core problem of today.

Those seeking to survive in a globally competitive world, have to put the conflicting demands of government and regulators into context. Ignoring them may mean running the risk of being shut down for non-compliance.

But taking them at face value could lead being put out of business by rivals based in locations like Switzerland, Singapore or Dubai, whose governments understand regulatory arbitrage.

The Corporate Balancing Act

Objective: organisational survival

- neither shut down for non-compliance
- nor put out of business by overheads

Demands Versus Needs

- Form 42
- Money Laundering reports
- Data Retention

Kafka (The Trial, The Castle)

v Hasek (The good Soldier Schweik)

Most demands for data from government and regulators are “in case”. They do not know what they may need to know to and do not appreciate that retained data becomes inaccessible or worthless unless it is actively managed. And active management is not only expensive, it also removes the evidential value of the data. We need to “educate” politicians, officials and regulators to find a better way.

“Form 42” refers to a classic example of an expensive and worthless state imposed overhead given to me by a member of the Public Accounts Committee at the time. This was a return of share issues demanded by the British Inland Revenue to avoid a particular tax avoidance risk. The financial services industry was unanimous that it would not address the problem but they were ignored. No routine had been set up to handle the forms so these were to be returned to Room X in Somerset House. Some years later Room X was full and no-one had done anything with the forms. Were they were finally shredded during the run-up to the Freedom of Information? Or are they still being collected and archived for posterity?

A more recent example concerns the routines for reporting possible money laundering. These place serious overheads on the innocent and swamp law enforcement with irrelevant returns but do nothing to hamper the guilty. Debates over the retention of communications data and e-mails are similarly surreal.

The need is to have processes in place to report, retain and analyse that of likely value, in time to take effective action. The American problem during the run-up to 9/11 was not too little data. It was the inability to sort the relevant and significant from the rest, before being overtaken by events. A paper by the EURIM E-Crime Working Group on the reporting of electronic malpractice concluded as follows:

“Much can be done to reduce fragmentation and duplication of effort with regard to reporting structures and improve the availability of intelligence to help focus existing resource. However, there remains a Catch 22 situation with regard to justifying the resources necessary to create easy-to-use reporting systems that will not be swamped. Without such systems we risk confidence in the Internet being eroded by the inability of most users to report incidents to someone who will take notice of their concerns. Education and awareness campaigns could do more harm than good unless accompanied by such routines.

In the mean time we have to live with current reality, including compliance paper-chases dreamt up by corporate bureaucrats and their legal advisors and other consultants.

The tangle of regulatory compliance and governance demands that you face is straight out of Kafka.

But before Kafka wrote *The Trial* (1925) and *The Castle* (1926), his fellow Slovakian Jaroslav Hasek had already identified the principles for handling bureaucratic uncertainty and complexity. *The Good Soldier Schweik* was published in 1922.

Not all the techniques used by Corporal Schweik in World War 1, or by his German equivalent, Gunner Asch, in World War 2, let alone those of their American cold war disciple, Sergeant Bilko, would go down well in your organisations. But we too have to be seen to obey the rules while not paralysing the business.

We have ensure good practice in a tempting environment, policed by bureaucrats, who are less concerned to deter, detect and correct malpractice than to ensure they cannot be blamed, whatever happens.

That requires you to work with your peers to ensure that governments and regulators produce relevant codes of practice and police them in co-operation, not confrontation, with those who share the objective of preventing malpractice, not just ticking the boxes.

Those codes of practice have to enable your business to implement front-line procedures that ordinary human beings can and will follow, which meet the needs of the business and its customers, while securely recording and archiving everything a regulator might need. That means they must not get in the way of customer service.

Users must not have to bypass security in order to do the job when and how the customer wants.

Practical Risk Assessment

The biggest risks are:

- Insiders: top management, IT staff, marketing, cleaners and untrained users
- Digititis: cock-up compromising or crashing “over-integrated” databases or networks
- Mother Nature: storm, flood, flu etc.
- Accident: fire, explosion

- Then comes outside attack
-

British IT users spend somewhere over £3 billion a year on systems security, most of it in protecting against outside attack. You might say that it is successful because all the evidence is that this is now the least of our problems. The billions lost by over-ambitious chief executives or a rogue trader dwarf the losses from any other cause save for mother nature - most recently all those IT-dependent firms put out of business when they lost their records in the recent West country floods in the UK.

I was, however struck by a recent survey regarding incidents which “compromised” information as opposed to costs or losses. The IT personnel were responsible for most. Marketing, the bete noir of most information security professionals, was actually a poor second.

One of the most interesting questions from the recent revelations regarding abysmal practice by major organisations, was why processes that were agreed and supposedly implemented several years ago had been ignored. The answer appears to be simple. The processes were too secret to tell anyone.

I refer on the slide to untrained users - because the failure to agree security processes that meet business needs, are fit for use by ordinary human beings and are communicated to all staff lies behind most serious data losses. Unless all staff are trained in what the policy means to the business and to them, the policy might as well not have been drafted in the first place.

Information Security as a Customer Service

- A consent driven cycle of trust and validation (akin to financial services)
- Publicly accountable 3rd party governance for statutory powers
- Cost, risk and liability assessment for trust and governance models
- Clear (and published) rules, responsibilities and liabilities for operational staff
- Rolling data validation programmes
- An over-arching strategy for the inter-operability of identities (personal and legal)

We hear much about information security being a cost or data protection being a problem. But they should also be seen as a great opportunity to improve customer relations, validate files and make new sales. Those who want the business of the “wealthy but cautious” need to find new ways of doing business - and being seen to take customer protection seriously may well be key.

The current plague of spam and phishing is leading to major changes in how reputable organisations use the Internet to contact customers and prospects. We need to use the pressures for reporting data losses to also cause organisations to stop placing cookies on the systems of casual customers, to call a halt to collecting unnecessary information and to drop password protection for that which does not need to be secure. The pay-per-click advertising bubble may also be about to burst because of fraud and abuse.

This approach also needs to operate across all channels. For example those manning call centres need clear instructions on how to politely check that the caller is entitled to the information - just as those receiving phone calls from what claims to be their bank need to be able to verify the caller. And call centres need to be seen as secure environments with staff and visitors checked, vetted and monitored.

Enquiry Chart

No policy has practical meaning unless and until all staff have clear training and guidance as to whom they can and should pass information, how to identify them and who to call when in doubt. This chart was developed by a EURIM sub-group to help discussions on how that process might work.

Once you have validated that the enquirer is genuine, the enquiry should be welcomed as an opportunity to update the file especially if it is the data subject wanting to know what is held about them.

At the same time as getting them to correct any errors, you can ask what they would like from you - whether to be left alone, or to receive details on something different to what you have been promoting to them.

Information Assurance as a Customer Service

- A consent driven cycle of trust and validation (akin to financial services)
 - Publicly accountable 3rd party governance for statutory powers
 - Cost, risk and liability assessment for trust and governance models
 - Clear (and published) rules, responsibilities and liabilities for operational staff
 - Rolling data validation programmes
 - An over-arching strategy for the inter-operability of identities (personal and legal)
-
-

Law enforcement agencies, regulators, auditors and others seeking access to customer or employee data should be routed to the organisations' security team, to check their credentials and to help them find what is really wanted. Corporate security staff should also be trained and accredited to use the same protocols for collecting and preserving evidence as their counterparts in law enforcement to enable full two-way co-operation in investigating and/or prosecuting serious malpractice.

This is a major thread in the EURIM work on the enforcement side of building confidence in the Internet as a safe place.

I will not go into detail on the other points on this slide other than to say they need to be addressed politically at both national and European level, with proper impact assessments for any new regulatory proposals. And you as Information Security professionals need to respond individually and collectively, including via ISSA, not just via your companies and their trade associations, if the results are to be better than the current muddle.

Slide 7

Fight Your Corner for Better (not more) REGULATION

Contribute through ISSA and its planned awareness programmes for directors and SIGN the Number 10

Petition - <http://petitions.pm.gov.uk/ecrime/>

For details of the EURIM work

Visit www.eurim.org.uk

Or e-mail virgo.phiiip@eurim.org

To conclude - if you want your organisation to survive and pay your pension, you need better regulation, not more of it. And that means being politically active. And you can begin with the easy bit - sign the Number 10 petition calling for urgent action on the plans for a national e-crime co-ordinating unit

Thank you for listening.