

To EURIM Members and Observers

From Philip Virgo, EURIM Secretary General
15 Chestnut Road, London SE27 9EZ
Tel:020 8761 5926; Fax:020 8670 4345
E-mail: virgo.philip@eurim.org

THE EUROPEAN
INFORMATION
SOCIETY GROUP

EURIM



EURIM Newsletter - June 2005

1) Briefing Material for the new Intake of MPs

Setting the agenda for the next Parliament

We happily welcome back almost all our pre-election parliamentary members but one of few we lost was, most unfortunately, Brian White MP, our Chairman. Brian is widely respected across the industry and we have received many expression of regret, including from active supporters of other parties. There is a widespread hope amongst Corporate and Associate members that he will be professionally active in helping some of the ICT industry players to be more effective at the political level. One of the motions at the Annual General Meeting on 15th June (members only) is therefore to give him Honorary Membership, not just to say thank you for all that he has done in the past, but also to encourage and help him with all that we hope he will do in the future.

Nominations can still be taken for the new EURIM Managing Council, to be elected at the AGM. Please e-mail the Company Secretary, Kate Norman, at eurim@eurim.org if interested. The other main item will be to discuss priorities for the year ahead. In the meantime, we are assembling material under the editorial direction of Ian Stewart MP, to help the new intake of MPs to “come up to speed” on some of the issues already facing them, or likely to do so in the near future.

The most immediate of these is ID Cards, where we will be aiming to put the issues into the context of the overall management of personal identity and data sharing, often between departments and agencies who do not trust each others data, systems or even people.

Linked to this are the pre-conditions for the successful delivery of public sector systems. Here we aim to focus on case studies illustrating how and why success was achieved, not the usual post-mortems on failure. Unsurprisingly the problems are usually people, politics and management, not just technology.

The third priority is to control computer-assisted crime and reduce on-line vulnerabilities: from Internet safety and child protection, through phishing and fraud, to handling the mountains of potential digital evidence now involved in investigation and prosecution of even traditional crime.

We also need to address Internet (broadly defined) content (equally broadly defined) and regulatory convergence. The BBC is the UK’s largest provider of Internet content. Mobile phones that can carry TV broadcast as well as video streaming are intended to be the teenagers’ “must have” for Christmas 2005. Students are already mixing material from all sources over the 100 meg LANS serving their halls of residence. Where does this leave some of the assumptions behind the creation of Ofcom?

In each case we will aim to work with and through our Corporate and Associate members and other partners, including those expected to run the relevant registered All-Party Groups, as and when these are reconstituted/restructured in line with the growing pressure from MPs and Peers to make better use of their time.

2) Setting the Forward Agenda for Personal Identity and Data Sharing

Towards secure and trusted data sharing

The personal identity group now has 180 participants from over 50 members and observers, including most of the central government departments and agencies with major programmes or policy responsibility, as well as most of the large suppliers, trade associations and professional bodies active in this space. It is, therefore, in a unique position to produce balanced material on those issues not already well covered elsewhere.

Much of the discussion at the most recent workshop, on 25th May, was on the need to place issues in the context of the drive to develop a national strategy for IT in the public sector for announcement in November 2005, and not just the immediate debate on ID Cards. The cost of failure to have accurate shared data available, when and where needed, can be measured in pain, suffering and even several hundred avoidable deaths a year. But the abuse of shared data can be similarly measured.

The public sector is not a centrally controlled PLC. Those at the top of the departmental fiefdoms were selected for their ability to manage political, not operational, risk. The mechanisms for cross-departmental co-operation are at best patchy. Many public servants have good reason not to trust the data or security, let alone systems, of their supposed partners, public as well as private. Moreover, the needs and applications for which data is held are as diverse as the management and governance structures, let alone technology implementations. But it is not practical to meet public expectations for better service, let alone deliver the Gershon agenda, without effective sharing

The group therefore agreed to address the need for protocols to cover not only authorisation and authentication (where we have already made good progress) but also provenance, reliability, liability and reporting, given that the management and governance structures and legal regimes, not just technologies and file structures, can be very different. A summary report of the meeting will be placed on www.eurim.org.uk in the working group area of the website.

Members' experiences during the general election indicated that the flaws in the register were every bit as serious as those revealed during our pilot exercise to compare publicly available name and address files with current reality, as discovered during door-to-door canvassing. Those involved in this exercise are meeting later this month to discuss a follow-up: perhaps beginning with an attempt to classify the reasons why less than 20% of the residents of a ward comprised mainly of century old housing were found to be on the current register. These are believed to go beyond the simple "churn" of students, contract workers, travellers and other "temporary residents", a factor which also needs to be better addressed if new proposals to tie identity to name and address are to be more successful than those in the past.

At the 2nd June meeting, the forward work programme will be reviewed in the light of recent discussions, including on the issues that need to be addressed in the ID Cards debate. The final meeting before the summer recess is provisionally scheduled for 14th July.

3) Rebuilding Trust in Public Sector Information Systems Delivery

Building on case studies of success, not post mortems of failure

The revised deadline for cases of success for inclusion in the initial round of material is 6th June. Cases need not only to illustrate how and why success was achieved but to be attractive, interesting, relevant to the audience and delivered when and where that audience finds convenient. We are particularly looking for those that have political messages, "to ensure that programmes are not doomed before they start by unrealistic assumptions with regard to timescales, resources, development and implementation strategies etc." The expectation is that the relevant professional bodies (such as BCS, CIPS, IEE and IMIS) and trade associations (such as Intellect and ISPA) will be working with and through organisations like the NCC to help eGU and OGC ensure the necessary professionalism at the user and supplier level. The EURIM contribution will, however, also entail close co-operation and full and active support from those with delivery responsibility. Those interested in active participation, particularly in volunteering to help produce case studies, should e-mail eurim@eurim.org.

4) Prioritising the Fight Against E-Crime

Apart from the issues of on-line child protection, computer-assisted crime does not appear to feature among current political or policing priorities. It is therefore important to begin by putting the issues into context. It appears to account for about 3% of the overall cost of crime but less than 0.01% of police spend. Meanwhile industry spends around 14.5% of its total security spend on protecting itself and its customers from attack. The £3.2 billion expected spend of ICT users on e-security this year compares to a combined expectation of £8.5 million for all the national and local computer crime units, including NHTCU and the new Internet safety/child protection unit and the other digital investigation support operations to be placed within SOCA.

Meanwhile ten per cent of the population of the world, including around 60% of that of the UK and a comparable proportion of criminals, are now on-line. Most conventional crime now requires computer skills in the course of detection and prosecution, including in the examination and presentation of potential evidence from the phone, organiser, computer or mailboxes of a victim or suspect or from the surveillance cameras or other devices covering relevant locations.

The implications for a society that is increasingly dependent on the use of computers in all walks of life are very significant and EURIM has been working with IPPR and around 140 representatives from over 60 organisations, public and private, to suggest how these might be handled within a coherent, cross-departmental, national strategy, as was announced in principle last year. Excluding obvious points on budgeting and resourcing priorities, the main recommendations to date have included:

- **Non-Geographic Reporting:** a national network to which “non-geographic incidents” can be reported, well-resourced in terms of equipment and processes as well as staff, which will collate reports and forward them rapidly to those responsible for action.
- **Cybercaddies:** non-geographic crime and disorder partnerships supported by joint law enforcement-industry investigation teams, using supervised and trained volunteers and specialists, and covering the different but overlapping communities concerned with child, consumer or infrastructure protection, as well as financial services or serious and organised crime.
- **Action on Skills:** (prevention as well as investigation), backed up by serious funding and ranging from basic e-security and e-citizenship (which should be mandatory on all publicly funded ICT courses and qualifications) to high level forensics skills.
- **E-crime prevention:** high visibility programmes linked to properly resourced reporting and support (industry as well as government).
- **Frameworks for co-operation:** with shared processes and protocols to facilitate joint investigations involving industry specialists and civilian volunteers, and legislative updating, including to the Computer Misuse Act, to enable more effective international co-operation.
- **International Co-operation:** the UK should use its Presidencies of the G8 and EU to harness industry expertise in the creation of effective cross-border processes.

We hope to meet with the Minister shortly to discuss how to help secure the political support that will be necessary for actions that cross departmental boundaries. In the meantime we plan to:

- summarise and prioritise existing material to help brief the new intake of MPs and research assistants and thus help set the political agenda and expectations for the new Parliament: including with regard to the budgets and time allocated to addressing risk reduction, prevention, reporting and investigation;
- discuss with others, such as ISPA and the Mobile and Digital TV Operators, how to handle illegal Internet content (including new generation mobile), given the limited ability of the UK to influence changing technology and regulatory models and boundaries around the world;
- address skills and training provision - from self protection through organisational security to investigatory and forensics: in particular, who, including which minister(s), department(s) agencies should lead and in which areas?
- open constructive debate on data (including content not just communications data) retention and security in the context of the full range of governance and legislative issues and initiatives (from data protection to Sarbanes Oxley), not just RIPA et al.;

and press for early action to:

- update the Computer Misuse Act to facilitate international co-operation by making offences potentially extraditable;
- pilot the use of specialist constables and industry volunteers in joint law enforcement - industry investigation teams.

5) The Challenge of Convergence

Last week, Mark Thompson addressed a Westminster Media Forum event, including on the plans of the BBC to reinvent public service broadcasting for the Internet Age. Almost no one from the Internet community was present when the UK's largest remaining digital content provider set out its stall. The day before David Cleevely and Jon Crowcroft had given an equally breathtaking vision of how ubiquitous broadband, mixed and matched over a variety of fixed and mobile networks, could destroy most current business and regulatory models well before the BBC charter next comes up for renewal. Almost no one from the media or content worlds was present.

As has been said before, "the technologies may be coming together, but the people are not".

Suggestion as to how to handle the issues, including regulatory convergence (applications and content not just infrastructure) in partnership with the other relevant interest groups would be most helpful.

To EURIM Members and Observers
From Philip Virgo, EURIM Secretary General
15 Chestnut Road, London SE27 9EZ
Tel: 020 8761 5926; Fax: 020 8670 4345
E-mail: virgo.philip@eurim.org

THE EUROPEAN
INFORMATION
SOCIETY GROUP

EURIM



EURIM Timetable – June 2005

This timetable lists forthcoming meetings arranged by EURIM and also includes some, arranged by other organisations, which are likely to be of interest to EURIM's Members and Observers.

Unless otherwise indicated EURIM meetings are open to all members and accredited observers. There is no charge for attendance but prior registration is required. If you wish to attend or would like more information please contact the named individual or eurim@eurim.org.

For information about meetings arranged by other organisations, please contact the person or website indicated against the entry. Note that for some events, there is an entry fee and pre-registration is essential.

June

Date: Thursday **2** June 2005
Time: 10.00 - 12.00
Venue: 1 The Abbey Garden, Westminster
Organiser: EURIM Personal Identity Group
Description: Meeting to review progress and make forward plans in the light of the outcomes from the recent meeting with eGU.
Attendance: Group members, observers & guests

Date: Wednesday **8** June 2005
Time: 13.30 - 17.00
Venue: Bird & Bird, 90 Fetter Lane, London EC4A 1JP
Organiser: E-business Regulatory Alliance
Description: Industry Round Table Discussions with DCMS and the Home Office
Attendance: Email will.roebuck@e-ra.org.uk or telephone 020 7905 6281

Date: Monday **13** June 2005
Time: 14.00 - 17.00
Venue: Hosted by Cisco, 12th Floor IFC, Old NatWest Tower
Organiser: EURIM E-Crime Group
Description: Workshop to draft grid of Internet Safety and Security Awareness Programmes in Schools
Attendance: Group members, observers & guests

Date: Tuesday **14** June 2005
Time: 11.00 - 17.00
Venue: Attlee Suite, Portcullis House
Organiser: PITCOM
Description: Exhibition for new Members
Attendance: MPs only

Date: Wednesday **15** June 2005
Time: 15.30 - 16.30
Venue: 7 Millbank, London SW1
Organiser: EURIM
Description: Board & Council Meetings
Attendance: Board, Council and invited guests

Date: Wednesday **15** June 2005
Time: 17.00 - 18.00
Venue: 7 Millbank, London SW1
Organiser: EURIM
Description: Annual General Meeting
Attendance: Members only

Date: Tuesday **21** June 2005 - Wednesday **22** June 2005
Time: All-day
Venue: Earls Court One, London
Organiser: Government Computing
Description: Two day Conference and Exhibition
Attendance: For more details visit www.gcexpo.com

Date: Monday **27** June 2005
Time: 18.00 - 19.30
Venue: To be confirmed
Organiser: PITCOM
Description: Update on NHS Connecting for Health: Richard Grainger, DG of NHS IT and CE of NHS Connecting for Health
Attendance: PITCOM members only: www.pitcom.org.uk

Date: Tuesday **28** June 2005
Time: 18.00 for 19.00 - 22.00
Venue: National Liberal Club
Organiser: Real Time Club - partners' evening
Description: Digital technologies, education and entertainment: after dinner discussion introduced by Lord Puttnam.
Attendance: E-mail carmen.harvey@e-skills.com for an invitation as a EURIM member.

July

Date: Thursday **14** July 2005
Time: 10.00
Venue: To be confirmed
Organiser: EURIM Personal Identity Group
Description: PI Group Meeting
Attendance: Group members, observers & guests

August

Date: Thursday **25** August 2005
Time: 10.00
Venue: To be confirmed
Organiser: EURIM Personal Identity Group
Description: PI Group Meeting
Attendance: Group members, observers & guests

September

Date: Thursday **8** September 2005 - Saturday **10** September 2005
Time: Three days
Venue: Saïd Business School, University of Oxford
Organiser: Oxford Internet Institute
Description: Major conference to address the value choices and conflicts surrounding cybersafety in a converging world
Attendance: For more details visit <http://www.oii.ox.ac.uk/>

October

Date: Thursday **6** October 2005
Time: 10.00
Venue: To be confirmed
Organiser: EURIM Personal Identity Group
Description: PI Group Meeting
Attendance: Group members, observers & guests

Date: Tuesday **18** October 2005
Time: 16.00 - 17.00 (provisional)
Venue: To be confirmed
Organiser: EURIM
Description: Board & Council Meetings
Attendance: Board, Council and invited guests