

**Minutes of Open Meeting of the EURIM Secure Electronic Commerce Group
held at 1 The Abbey Garden, London SW1 on 29th June 1999**

1. INTRODUCTORY

- 1.1 The Chairman explained that the meeting had originally been convened as a briefing on the electronic commerce bill - now apparently called the electronic communications bill - but publication of this had been delayed. Discussion would now focus on a number of surrounding issues with particular emphasis on consumer protection.
- 1.2 Philip Virgo gave a round-up of current e-commerce initiatives in UK, Europe and the US, with an indication of where they fitted in and what EURIM should do.
- 1.3 UK initiatives included:
- 1.3.1 A major cabinet office exercise to produce a report on things needed for e-commerce. Was this the brief for the e-minister? There was nothing tangible on his appointment.
- 1.3.2 Electronic communications bill - covering, writing and authentication - and perhaps with reserve powers for a licensing scheme
- 1.3.3 Review of IOCA, now a separate bill - aimed at bringing it into the Internet age.
- 1.3.4 Review of criminal law - EURIM was holding a workshop on 12 July which would look at electronic fraud, impersonation, and areas where definitions in criminal law were now out of date.
- 1.3.5 Implementation of Telecoms Data Protection Act - includes rewrite on distance selling - opt-in and opt-out - how to administer it? Who to do? Fees?
- 1.3.6 Implementation of Data Protection Act. 6 of the instruments were up - regarded as the most boring and least controversial. There were 26 more to do and some would be debated on the floor of the House.
- 1.3.7 Electronic commerce was in the hands of the DTI as they sponsor the suppliers. CST have music etc., while the Home Office protect from naughty things.
- 1.4 Current initiatives in EUROPE included:
the electronic signatures directive;
the directive on the distance selling of personal financial services;
the electronic commerce directive
the copyright directive.
Whereas the first two were progressing reasonably smoothly, the latter two were both stuck firmly in the treacle. The problem was exacerbated by the number of different DGs with an interest in the affected areas - principally III, IV, X, XIII, XXIII and XXIV.

- 1.5 In the USA, it was recently decided that matters of e-commerce were for consideration by state, not federal, courts. Consumer protection and privacy were already regarded as state matters. Some interesting cases and decisions have resulted, eg some banks have been prevented from selling information to third parties.
- 1.6 Technological developments were providing solutions to many of the issues. SET was expensive to operate and support and Visa and Mastercard were both looking for token based solutions. There was a proposal that financial firms should get together to regulate net trading. They would form an OnLine Finance Association and establish codes of conduct.
- 1.7.1 Consumer confidence was essential for the success of e-commerce. UK businesses needed to set standards and to adhere to high standards. Consumers needed advice and education.
- 1.7.2 A National Consumer Council report showed that 11% of all orders backed by credit cards were not delivered although the charges went through. They estimated that 70% of transactions over the Internet failed.
- 1.7.3 Figures quoted on card fraud could be confusing. Fraudulent card-not-present recharges accounted for less than 10% of the total paid out by banks.
- 1.7.4 The Government were producing this bill to overcome fears and build confidence. It remained to be seen if, in this environment, that would be the effective way forward.
- 1.8 *Kite Marks*
- 1.8.1 The Consumers Association launched their kite marks 10 days previously, with several traders already accredited. They are designed for sales in the UK by UK organisations. A key requirement is that there are no hidden costs and that a delivery date must be agreed and a firm price given. The requirements of the Advertising Standards Authority and Sale Promotion Code must be met. Contracts must be in clear and plain English, with UK as the applicable law and the terms must be easily found on the trader's site. The kite mark will be monitored.
- 1.8.2 The Alliance of Electronic Business (FEI, CSSA, CBI and DMA) have agreed to try and create an umbrella organisation for UK kite marks in general to promote the UK as a safe environment for doing business.
- 1.8.3 It was alleged that in the USA, 70% of kite marked traders were not complying with the markers' codes. Watermarking of kite marks was being proposed.
- 1.9 The other side of the coin was that small firms putting their business on the web need assurances that they will be paid. Many believe that getting credit card details guarantees payment, but there are many repudiations.
- 1.10 EURIM's e-commerce working party was examining the barriers to e-commerce.

- 1.10.1 The Network governance working party was concerning with the pre-conditions for effective self-regulation. They were also looking at the regulation of financial services.
- 1.10.2 The IPR working party was looking at intellectual property rights where rightsholders want to be paid for things that are downloaded.
- 1.11 The government's own use of e-commerce spans all the problems.

It seems that only part of these things will be addressed in the electronic communications bill that we have not got. Other things are muddled and confused and there may be no prospect of coherent legislation. Industry must find de facto frameworks that will give people confidence that what they are doing is legal in the markets they are trying to address and that consumers do know what they are doing when they double click.

2 DISCUSSION

- 2.1 IB indicated a need to concentrate on determining where legislation was actually needed. Many of the problems reported in the context of e-commerce were already covered by existing law. For instance, current law is clear on fraudulent transactions, which includes giving an incorrect credit card number, so we don't need new legislation for that. Too often when the law is changed it proves ineffective because its terms cannot be enforced. How to enforce existing law is often the bigger problem.
- 2.2 NP considered that the problems can down largely to confidence. There was unease on the consumer side about give card details over the net, although that was probably not justified. It would be useful to industry if popular confidence in the process could be strengthened. Despite unease, many vendors are steaming ahead, although maybe not as fast as they would like. The US trend was probably a guide to us. He felt there was no compelling political reason to have lots of new laws on this but hoped to get an impression from the meeting of what might actually be needed. There was a real vacuum in the creation of de facto standards which can then be used by legislators as the basis for compliance. There was an opportunity here for industry here as there was a considerable overlap of interest between responsible vendors and responsible legislators.
- 2.3 RT commented on the contrasting amount of progress in different areas. Of particular importance in the UK were issue of:
 - 2.3.1 Liability - there were many long-standing bi-lateral agreements and it was important not to upset existing contract based customer practice.
 - 2.3.2 Lawful access was not going to go away. Key escrow was dead, but there was a real law enforcement issue.
 - 2.3.3 Regulation - he was pleased to see MW talking about co-regulation. He suspected MW was the only person who knew what he actually meant, but it was acceptable as a sound bite! If it meant a number of stakeholders, the only way to grow the

market was, he said, for BT to carry them with them. The regulator needed a valid and loud voice in all this, but running it from Whitehall would only perpetuate the mess.

- 2.3.4 He had some reservations about the electronic signatures directive. The definition of a qualified electronic signature required the use of smart cards. This was too narrow and if made essential it would raise the costs of entry - smart card readers were not cheap. Many security mechanisms would be suitable for most transactions. He noted the close match between the directive and the German digital signature law. A forthcoming meeting in Brussels would discuss a report on how to implement the directive - at 90 pages long, it indicated the complexity of the subject.
- 2.3.5 The OECD was currently looking at authentication and it would be worth keeping an eye on this. While Europe was focusing on legal recognition, the US was just getting on this doing things. The OECD was where these two camps met.
- 2.3.6 Asked about issues relating to debit cards and to mobile phones, RT indicated that these were not legal issues but ones for systems designers. It was, however, important that there was general recognition of the differences.
- 2.4 ST, in explaining that he was not an expert on cards, spoke of two important issues: Firstly, how can we best use existing systems in today's environment and, secondly, what would be better mechanisms?
 - 2.4.1 The credit card was originally designed to be used at point of sale. It worked best when a physical card was in an individual's hand. The Internet is one more type of card-not-present transaction. Debit cards are not covered by consumer credit law. So if there is a reason not to pay, the risk is borne by the merchant. Cards are used for payment because that is the easiest - not necessarily the best - way of doing Internet payments - Something using a 3 day clearing cycle is not attractive. There are no answers yet.
 - 2.4.2 Regarding the use of electronic signatures, the key element was not the technology but the business model on which the e-commerce system was built. There is a fundamental flaw in model as the person who needs to rely on the signature is the recipient who has no association with the certification authority. There need to be inter-bank guarantees
 - 2.4.3 There was no doubt that card fraud on the Internet did happen - however, it was not done by "eavesdropping" during the transaction; but more likely by getting at merchant's lists. Also there was software to generate false but plausible credit card numbers. Fraud data was collected but it was difficult to determine where the point of compromise was. Looking at evolution of fraud figures over the last five years, the percentage of credit card fraud has greatly increased. We are gradually getting chip cards but retailers are slow to adopt readers.
 - 2.4.4 SET is a heavyweight and has not been a success. It attempted to give credit card number information in a secure fashion and keys were stored in software on a PC, so the user was tied to a single machine. The capabilities of chip cards would deal

with that problem - but that is several years away.

- 2.4.5 NP - We already have several levels of security and one difficulty is trying to make one size fit all. Is it in the industry's interest to offer different degrees of security for different risks? We could encourage the use of chip cards by saying that in that case the bank would take over all or much of the risk.
- 2.4.6 ST - That is certainly feasible. There are arguments on what is a legally admissible electronic signature. There are some parallels with the use of PIN numbers.. Different levels of usage and liability are possible, but not different levels of legal admissibility.
- 2.4.7 PV - Authentication authorities can say this is a valid signature of this person, but that person may be a fraudster. So it does not say that the person is good for the transaction and the amount involved.
- 2.4.8 ST - The on-line authorisation model is very complex
- 2.4.9 IB - One can understand a vendor can get a more complex package to use but to be sure does he not need an interactive transaction?
- 2.4.10 ST - not necessarily - but refreshing is required. The signature is different for each document signed - if the document changes a new signature is always needed and this can only be done from the signatory.
- 2.5 RW returned to the e-commerce directive, which had the objective of creating a coherent structure for e-commerce in the community.
- 2.5.1 Real flow of e-commerce at the moment, he said, was still business to business. Europe was trying to create its own Utopia despite the global position. Provisions within this directive for creating a contract differ from those of the parallel distance selling directive. There was no need for the difference. Consumer protection was supposedly for national governments - in both financial services and general directive. The definition of financial services was so wide that it could trap any transaction not requiring immediate payment in full.
- 2.5.2 Caching, etc ,doesn't conform with the current environment, so why introduce the issue as it won't be tomorrow's technology. Clauses are based on the draftsman's ;understanding of the technology, which is rarely accurate.
- 2.5.3 On the consumer side, the barriers have nothing to do with government. An example is the time lags in Internet banking, which is currently very slow. The design of sites is often desperately unfriendly - this is bad management. How do you create confidence in a consumer? Not just with kite marks. How to educate them? Where do they go to get information? Some of this could be provided by the ISP when they first subscribe.
- 2.5.4 Ultimately, who is going to protect the consumer? The country of supplier or the country of consumption? There are different schools of thought on this. He considered that the country of consumption was the only practical one and that the

- EC approach did not make sense.
- 2.5.5 NP -It seems that regulating by the country of consumption creates an impossible position for the vendor, who can reasonably be expected to cover rules made in his own country but not in 119 others. Caveat emptor must apply. This is intuitively what most people would expect.
- 2.5.6 PV A unique UK strength is that much global trading expertise is here, especially freight forwarding around Heathrow . For it to adapt to electronic needs is a UK opportunity not a problem. Offer as part of ISP or bank service to trader.
- 2.5.7 IB - international jurisdiction is the most difficult and most crucial matter for government. It can only work if there are international treaties. In many cases you don't know where you are buying from. We ought to be looking at what HMG is doing in terms of international treaties and whether they would upset existing codes of practice. There are real legislative issues - eg BT can't deny access to known crooks.
- 2.5.8 CW - if people can use flags of convenience for internet addresses, they may not be well respected. Some countries will not sign up to treaties. Also company doesn't know where the consumer is - either based or temporarily. Unless delivering to a physical address they cannot find out.
- 2.5.9 PV -Harmonisation of VAT and G8 things on tax are relevant here. Who is liable to whom for collecting valid taxes? Tax authorities are driving hard with rules for a different community - but need to be linked in to other aspects.
- 2.5.10 RW Current users are largely sophisticated techno freaks. As time goes on the balance will change and many more physical things will be delivered, so consumer location will be known relatively more often.
- 2.5.11 NP Is there public interest in people being able to represent themselves as being in a country where they are not? Credit cards are linked to an address; could ISPs be required to provide this information?
- 2.6.1 CB - Plea that when bill reaches committee stage MPs recognise that they cannot understand anything in it unless they understand the basic principles of public key cryptography; which have counter-intuitive aspects at its core. He urged the committee to spend 40 minutes on a tutorial.
- 2.6.2 (IB - a bill committee formally cannot do that but the individual members of the committee can certainly do so.)
- 2.6.3 Credit cards were important at present but we must look ahead to electronic cash. There are problems for new entrants to get merchant status - need 3 year history etc. (was this a UK specific problem?)
- 2.6.4 OFT was more suitable as watchdog than OFTEL if a regulator was required. This would demonstrate that consumer protection was the main issue.

- 2.6.5 The Directive was a miracle of bureaucratic engineering. Look at the definition of a qualified certificate - does this actually require a smart card, which will not be standard in PCs for a long time. Nordic tendency in the EU happy with an identify card approach and Anglo-Saxon reluctance of it.
- 2.6.6 He had reservations on European standardisation initiative. Quango of closed groups.
- 2.6.7 He considered there was a breakdown in co-ordination - It was UK policy to beaver away at export controls on intangibles. Now key-escrow had gone away, there was no need to extend cryptography legislation to intangibles. Software has to be remotely maintained and cryptography provided a means of doing this. It was not practical to get a licence every time support was needed. Removing the controls altogether, however, was not acceptable to the USA.
- 2.6.8 Decryption warrant - where will the onus of proof on whether it can or can't be done lie? It doesn't follow that the person who knows how to encrypt something also knows how to decrypt it. The level of understanding in the Home Office are still extremely poor - there is not one official who is technically competent in this area.
- 2.6.9 For several years Liberty, Justice and now DPR have called for judges to issue interception warrants. The Home Secretary has personal responsibility to scrutinise - now doing 2K a year - must be processing about 25 some days. The current level is already straining credulity - exponential rise since 1945. Situation has worked well since its introduction but those investigating are judges not technologists. Lawful access issue won't go away and it is incumbent on industry to follow up - must walk fine line between cooperating and being suspected of building in back doors.
- 2.6.10 The legal judgement against demon ruled that they can and must implement the notice served on them to remove defamatory material? But the ruling depended on ISP's technical ability to remove the material, not any other issues. It should in fact be a notice to block, not notice to take down. It was considered legally damaging if that was carried through. There should be common carrier exemption
- 2.7.1 JP - ISPs could be regarded as a class of the community in the e-commerce society and thought be given to what is needed to safeguard their interest. Consumer protection is difficult as situation changing so quickly. Industry response in terms of brand building to inspire confidence - need help to build confidence as concerted effort between traders, banks etc.. Look at all the players and see how to co-operate. Would be nice if a very lean bill - like no bill at all.
- 2.7.2 NF - The BCS- should legislate for public key infrastructure and set out standards - this would help to create public confidence.
- 2.7.3 MR - agree about OFT being the overseer. Consumer confidence is at the heart of this. We can't second guess what is happening but must get it right this time. We need enabling, not disabling legislation. We need to watch the EU as much of

what they are doing is disabling.

- 2.7.4 DE - It is open standards that will make e-commerce succeed. We must cover security and get round to trust and credibility. We will end up with having to have some sort of TTP. How do you trust the TTP - by regulation or by self regulation? Either is OK, but something must exist. There is a need to cover establishing liability. Contract law doesn't cover every situation - especially global ones.
- 2.7.5 PV - Why does the normal liability waterfall not apply? How much is legislation needed to clarify this or does existing off line law cover what is needed? Merely resist making on line liability less than that off line.
- 2.7.6 DE -We are dealing with new concepts. In e-commerce and using cryptography different chain.
- 2.7.7 KC - Services regulators - sign up to ICSTIS model and have a contract which shows where liability is. The code works. In e-commerce we need to do a lot at industry level. Make sure consumer is aware so that they can make an informed decision. Those with well known brand have a huge advantage.
- 2.7.8 IR - We need to think very carefully at what anything in the bill is seeking to address .
- 2.7.9 ST - what could government most usefully do to generate confidence? The answer is simple - use it.
- 2.7.10 IB - there is a definition within the computer misuse bill of electronic media.
- 2.7.11 CB - An enormous amount of work will be needed on the secondary legislation as that is where the detail will appear. It would be nice to think that key escrow could not be resurrected without new legislation.
- 2.7.12 NP -There is an element of a problem between industry and the politicians. Industry suspects politicians want to make life more difficult for them. Strong libertarian wing and on politician's side there is fear of ill-understood technology and they think they are being taken for a ride by people who won't provide adequate protection. Industry is saying leave it to us although we don't quite know what we are doing. I don't like the principle that ISP not liable for anything it transmits.
- 2.7.13 CB The problem is that ISPs do have some legal liability but there is no practical way of dealing with it.
- 2.7.14 CW They can have secondary liability. Services would be very expensive if mechanisms had to exist to enable monitoring and blocking.
- 2.7.15 BT - Internet Watch Foundation could have more force in law and enable ISPs to have defence of best effort.
- 2.7.16 PV -There is a contrast between ISCSTIS and Internet Watch Foundation. ISCTIT

have vastly bigger budget and simpler task. Few ISPs claim to be near common carriers - they offer a raft of services. Liabilities must match what is being provided.

2.7.17 CB - do we really want to go down the road that says ISPs must act as censors?

2.7.18 PV - Every corporate system is in a sense an ISP. This opens a can of worms.

2.7.19 CW -Refer to time stamping service - should that person be liable for the messages he time stamps?

2.7.20 IB - Internet was set up with a situation that allows information to be placed on it anonymously. Decision on whether one should always be able to trace back to a geographical location. Eg can avoid ICSTIS if sex lines use a non-UK telephone number. Call does not necessarily go to the physical location of the number dialed. Law exists in many individual jurisdictions to deal with the problem - IF they can be found. Need provision so that have to know where you are.

2.7.21 KC - ICSTIS do monitor international services.

2.8 CB - Identification is another difficult technical area and need to caution against using common sense. Short of issuing everyone with smart card as ID, there is no simple mechanism. Internet evidence trail via radius law. Technologies coming along which will make it even easier to be anonymous on the Internet. Home Office have shown no interest in this - probably because they don't understand the issue.