



**Report of the meeting of the E-Crime Group, Tuesday 9 September 2004, at 1000-1200 hours in Room 'N', Portcullis House, Westminster, on Legal Issues**

**SUMMARY OF MAIN POINTS**

1. The aim of the meeting was to review the recommendations of the EURIM-IPPR working paper 'Partnership Policing for the Information Society – Legal Issues' in the light of the All-Party Internet Group (APIG) report on the revision of the Computer Misuse Act (CMA). Both documents should be read alongside this report. They can be found at: <http://www.eurim.org.uk/activities/ecrime/legal.doc> and <http://www.apig.org.uk/CMAReportFinalVersion1.pdf> respectively.
2. The APIG report on the revision of the CMA and some related issues afforded the group the opportunity to identify those issues requiring political action so that they can be debated in the public domain in time for a ministerial announcement on the National Strategy. It is intended that key points from the papers will appear in party manifestos, which will change the status for ministerial and departmental briefs.
3. The group's response to the APIG report should be:
  - to welcome its recommendations;
  - to point out that their recommendation for 2 years (rather than the 5 years proposed in the EURIM-IPPR paper) is acceptable given that the context of the arrestable offence is being changed;
  - to pass comment on the need to consider the issues around recklessness (both with regard to perpetrating an attack, and in the context of the innocent but ignorant third party); and
  - to support moves to encourage private prosecutions by companies.
4. One of the most serious threats to corporate systems now derives from the way in which patches and fixes are reverse engineered into viruses and other attack tools before implementation by most large users. This needs to be addressed within the group on Reducing Vulnerabilities.
5. In the context of 24 by 7 international law enforcement-industry cooperation, there is a need for effective frameworks for ISPs to receive and respond to reports of fraudulent and illegal content from known "reliable" sources separately from their mainstream abuse@ routines.
6. ISPs could play an important role in combating spam by reporting incidences to the Information Commissioner for action under the new "desist" routines whereby repetition the actionable offence. This will, however, require processes that do not at present exist.
7. There is a good case for the UK to take a lead on Government-Industry cooperation on track and trace etc. with the aim of making it the internationally recognised centre for co-operation on policing generally. Although this is an ambitious aim, with implications for Home Office, DTI, FCO and law enforcement, and for UK positioning within the G8, it is consistent with DTI objectives for making the UK the best place for e-business.

## **1. Introduction**

1.1 The meeting was a sequel to the EURIM-IPPR Crime Study meeting in December 2003, which had led to the working paper 'Partnership Policing for the Information Society – Legal Issues'.

1.2 The aim of the meeting was to review the recommendations in the working paper, in the light of the All-Party Internet Group (APIG) report on the revision of the Computer Misuse Act (CMA) and some related issues. The need now is to define what issues should be addressed, in particular those requiring political action, so that they can be debated in the public domain in time for a ministerial announcement on the National Strategy. It is hoped that this will be made by early next year, but in any case before the General Election. It is intended that key points from the papers appear in party manifestos, which will change the status for ministerial and departmental briefs.

1.3 The current set of e-Crime meetings afforded an opportunity to update the work done so far, and should lead to the publication of discussion papers and recommendations by October or November. There is now a revised action plan from Skills for Justice following the EURIM meeting on 7 September; volunteers for the steering group must be employers who can define the skills needed in recruits.

## **2. Comments and discussion of paper**

2.1 Paragraph 11 of the APIG report on the CMA states that APIG found no evidence that the time limits imposed for bringing charges for s1 offences need to be altered. However, the time limit had caused a failure of a prosecution, and although there have been no direct discussions on raising the threshold for s.1, there is scope for change.

2.2 With respect to the threshold for the s1 offence, Home Office preferred a two year penalty (rather than the five years proposed in the EURIM-IPPR paper) because no evidence had been presented for raising the threshold above this. The problem encountered by the CPS and law enforcement agencies is that there is no 'serious arrestable offence' under s1, and therefore ancillary powers are not available. However, there is an ongoing consultation with the police that is likely to change the nature of what constitutes an arrestable offence and the ancillary powers such as search procedure that would be triggered. The results of the consultation are expected to be rapidly incorporated into the legislation.

2.3 The meeting referred to the notions of intent and recklessness in paragraph 67 of the APIG report, and considered whether there was value in extending any of the CMA offences (e.g. under s.3) to include recklessness. Much of the damage caused to computer systems by those who engage in malicious activities is unintentional and therefore reckless.

2.4 Persons who host the zombie could be considered reckless, but here intent is shown by the person who releases the tool; is there any ground for making the reckless host prosecutable? A number of factors were pertinent here. Firstly, the mental state (mens rea) of 'guilty mind': the zombie host may be unaware of its status. It could be argued that there is a corporate responsibility where systems have not been adequately defended.

2.5 There have been calls for action where a customer hosting a zombie machine fails to take action after their ISP informs them; however, this was a 'can of worms'. In such circumstances, it should be available to the ISP as part of the customer's conditions of service to disconnect the zombie host and inform others. APIG reported on this as a contractual matter, but the holding of a central database might raise data protection problems.

2.6 A UK firm that installed a company's telephone system and failed to close certain ports that a hacker was subsequently able to use to reroute the calls provided an example of a successful civil case of liability through recklessness. The company successfully sued the installer for breach of reasonable care, and thus set a precedent for similar actions. The meeting applauded the recommendation of encouraging companies to bring private prosecutions, and suggested that steps are taken to improve awareness of this. However, Home Office is not attracted to 'recklessness' as an offence in itself; there is a need to demonstrate intent, but discretion is also available to the courts.

2.7 Problems arose because of inadequate terms of contract, for example where a supplier undertakes to provide adequate security software – a system was not adequate when it failed. The

problem is the lack of quantitative measures, although this had been offset to some extent by duties of care. Another measure is general practice in the industry; where this is insufficient, liability can lead to damages. An example was also given of how guidelines issued by NCC Microsystems had been used as evidence of industry practice in a court case some years later. A statutory mechanism is now available in BS 7799, the code of practice for information security management.

2.8 Good practice is given by an 'adequacy' statement and BS 7799/ISO 17799, but these are not granular enough for setting up a meridian or a router. Common practice is not best practice - there are objectives but no controls, and detailed guidelines are needed. However, 'adequate' practice (that necessary to avoid being sued!) would be a great improvement on what commonly happens. EURIM had had a 'Fair Dealing' working party looking at contracts and fair terms, but it proved totally impractical to bring the various players together to agree anything meaningful. However, the embryonic strategic supplier relations group Jericho, set up in part because a number of users were dissatisfied with the products and services available from their suppliers, may also provide a point of leverage for inserting good practice terms into contracts – making this a civil or contractual issue, rather than criminal. CIPS might be approached to look at similar actions.

2.9 One of the most serious threats to corporate systems now derives from the way in which patches and fixes are reverse engineered into viruses and other attack tools before implementation by most large users. This needs to be addressed within the group on Reducing Vulnerabilities.

2.9 The group's comments on the APIG inquiry into the Computer Misuse Act should be:

- **to welcome the recommendations;**
- **to point out that their recommendation for 2 years (rather than the 5 years proposed in the EURIM-IPPR paper) is acceptable given that the context of the arrestable offence is being changed;**
- **to pass comment on the need to consider the issues around recklessness (both with regard to perpetrating an attack, and in the context of the innocent but ignorant third party); and**
- **to support moves to encourage private prosecutions.**

2.10 The meeting then considered the issues covered by the Group that are not in the APIG report but needed further comment or revision, and whether any new issues should be addressed. The meeting agreed with the APIG recommendation that the Law Commission expedite their work on the Misuse of Trade Secrets so as to develop a suitable framework to adequately criminalise the unlawful 'theft of data', but stressed the need for urgency here as the current situation disadvantaged UK plc.

2.12 Some believe that there is a degree of irresponsibility by industry on security issues – this is manifest in the proliferation of worms. Investigators find it difficult to elicit information from people, and data is not readily available even with cooperation. ISPs can be very difficult to deal with, giving varying responses according to the ability and determination of the investigator: this may necessitate a legal obligation on ISPs, backed up by a process or code of practice, to act in accordance with the law.

2.13 An alternative view held that ISPs can only become responsible for a problem when they become aware of it, e.g. the reporting of illegal images hosted by them. This issue might be better dealt with in the EURIM 'Reporting' workshop; reporting could be to ISPs as well as law enforcement agencies. In the context of the need for 24/7 international law enforcement industry cooperation, there is a need for a framework for ISPs to listen and respond to reports from "reliable" sources separately to their mainstream abuse@ routine. The British Computer Society's Security Committee might wish to follow this up – how should different audiences report illegal and harmful content to their ISPs? There is a need for guidance as to what (including what supporting information) to report to where and how to provide evidence that the reporter is reliable and well-informed.

2.14 An exercise in due diligence might be useful for ISPs. It is too easy to get an Internet account, and there is now a need for some kind of public record check, especially for 'Pay As You Go', where there should be a need for an individual to register and be identifiable. However, one way BECTA offers protection to children is by not giving them individual accounts – so that they are deliberately untraceable, and cannot receive emails from dubious people. But this also has the effect of making them untraceable when they indulge in mischief.

2.15 Perhaps there should be some kind of identity check as a recommendation before an account is opened – e.g. number and postcode. However, the EURIM Personal Identity Group had received evidence that there are a large number of addresses held on file that do not exist – streets of houses that have been knocked down are still held on address files. So the bad guys could easily use one of these addresses. The use of internet cafés and wireless also facilitated avoidance of registration. A range of measures may therefore be necessary to provide traceability without loss of private freedom, although some business plans have no traceability checks.

2.16 Track and trace can be subverted unless some mechanism for ID authentication is requested. Would this be a suitable recommendation for legal action, or should we suggest that ISPs offer it to customers as an online equivalent of ‘I don’t accept anonymous calls’? It was pointed out that most systems have blacklisting or blocking options, e.g. SpamHouse, and UKERNA has used similar IP-address blocking techniques. Regarding registering phone numbers and IP addresses by email for VoIP, a ready authentication solution is to ask the phone company to check the account against a name.

2.17 Claiming not to be someone you are is illegal in both EU and US jurisdictions, but spammers in the USA no longer even bother to hide their identity – the law is weak and not enforced. It was agreed that there needs to be greater awareness of this, and for companies to take action on behalf of their customers. Although technical solutions are increasingly available to counter viruses, spam is not always easy to detect. There have been discussions about pooling information on major spam incidences, but spammers are innovative and their messages can be unique and not easily recognised as such by a computer system. However, ISPs are perfectly placed to help, because by informing the Information Commissioner of its occurrence, so that he can use his “desist” powers they can ensure that the actionable offence becomes not “just” spamming, but repeating the action.

2.18 Members present were requested to check the EURIM-IPPR paper and identify what should be updated and our priorities for action, reporting back by the end of September – the aim is to have all the e-crime papers rewritten and circulated by the end of October 2004. Regarding RIPA, Home Office had indicated that the time is right to take another look at legacy powers, powers to claim data etc. It was noted that the recommendation on the Sexual Offences Bill was badly out of date.

2.19 We need frameworks for cooperation with regard to law enforcement and international aspects. Together with Home Office we should call for more effective, 24/7 Government-Industry cooperation to be a G8 objective, especially with regard to the frameworks on track and trace. Although prospects for agreement between Russia and USA with regard to subsequent enforcement by law enforcement are unlikely, Industry cooperation frameworks could lead to action. Another line worth pursuing might be to see if Ehab Elsonbaty’s ideas could generate plans for broader cooperative group action via a UN convention.

2.20 London’s position as the ‘ADR capital of the world’ was noted, and it was suggested that there is a good case for the UK to take a lead on Government-Industry cooperation on track and trace etc. with the aim of making it the internationally-recognised centre for co-operation on policing as well. The Economic Development Unit of the Corporation of London might be a good place to start the planning, but there are implications for Home Office, DTI, FCO, law enforcement and UK positioning within the G8. This may require inter-agency collaboration by 3 communities: ISPs (to remove bad traffic in their common interest), the financial community (big business involvement) and the legal criminal-law community (hardest to harmonize). Such plans are very ambitious: there would need to be absolute clarity about aims and how to achieve them. However, the aim is consistent with DTI’s objectives of making the UK the best place in the world for e-business

### **3. Conclusion.**

3.1 Participants undertook to report any further comments on the paper by end September.

3.2 The meeting closed at 12.00

### **Appendix 1**

This grid was drafted during the meeting as an attempt to summarise the four types of Internet abuse of current concern to UK citizens, the legal position, industry views and the actions under discussion.

<b>Issue</b>	<b>Legal status</b>	<b>Industry status</b>	<b>Action under discussion</b>
Phishing	May be covered by law, but draft Fraud Bill would clarify the situation	Unlikely that there is a technical solution to the problem, unless banks move to non-reusable authentication. Phishing web sites can be taken down by hosting ISPs but tend to change location rapidly (anecdotally at 5 minute intervals), giving this only limited effect.	Raise public awareness of threat
Viruses	CMA 1990 seems adequate for prosecutions in this area	Effective anti-virus software and services are available to customers at all levels.	Raise public awareness of threat and possible solutions.
DoS attacks	May be covered by CMA 1990 depending on details of technique used. APiG report recommends creation of a specific offence.	Technical prevention of attacks is almost impossible; cooperation between UK ISPs is improving to mitigate the damage caused by attacks, but action to block attacks is likely to also block some legitimate traffic.	Raise awareness of threat (especially of end-user machines being compromised and used in attacks). Efforts to identify and prosecute perpetrators are welcome but could be increased.
Spam	Current law (DPA1998 and Privacy and Electronic Communications (EC Directive) Regulations 2003) is weak, making only breach of an enforcement notice a crime.	A variety of services are currently available that achieve the best performance likely to be possible by solely technical means. UK ISPs generally take prompt action against their customers who send spam: the vast majority of messages received in the UK now come from overseas. Industry efforts to pressure overseas networks have led to threats of legal action.	International co-operation is needed to prosecute foreign spammers. Recent announcement of an agreement between UK/US/Au is welcome, but needs to achieve results to be credible. Raise public awareness of solutions and precautions.