



THE EUROPEAN  
INFORMATION  
SOCIETY GROUP

EURIM



## EURIM – IPPR E-Crime Study Partnership Policing for the Information Society

### *Working Paper 6: Legal Issues*

#### **The Issues**

The digital world presents a fast-changing environment with many unfamiliar aspects. It places particular challenges onto legal systems, which find it difficult to cope with the rate of change of this new world. Technical innovation continues at breakneck speed, people (including criminals) make innovative use of its capabilities, geographic boundaries become less well defined (creating jurisdictional problems). If the growth in e-crime<sup>1</sup> is to be contained, we need the law to become better adapted to this new environment.

The urge to create new laws to address criminal activity in this intangible world is great, but must be resisted. Popular demand in reaction to specific incidents (for example, paedophilia) can create an atmosphere where such laws appear to be necessary. Sober assessment of the true situation most often shows that the underlying crime is recognised as such, but that current laws and regulations effectively prevent prosecution of the crime when executed in the intangible world. The remedy is to remove impediments to prosecution under existing laws not, for example, to invent new, Internet-specific, laws. Only where there is an overwhelming case that a specific crime is unique to that world should new law be created.

Whether existing laws are amended, or new laws created, two further issues need to be considered. The digital world has the potential to enable ever greater intrusion on, and control of, members of society by government. It is also a highly complex technical world under constant change. The need is for laws and regulations to be written in ways that are technically neutral (thus reducing the need for continuous amendment as technology evolves), mutually consistent and sufficiently well defined to maintain an acceptable balance between the needs of the state to protect society, the freedom of the individual and the ability of organisations to take reasonable steps to reduce risk. That this is a difficult balancing act is shown by the ongoing debates over the Regulation of Investigatory Powers Act (RIPA) and Part 11 of the Anti-Terrorism Crime and Security Act (ATCS), and initiated by Chapter 4 of the recent Consultation Paper on Access to Communications Data.

E-crime does not respect national boundaries, requiring unprecedented co-operation between law enforcement agencies. Investigating and prosecuting cross-border e-crime highlights the differences between legal systems, cultural attitudes and social practices. Jurisdiction becomes a major issue. UK law has to recognise this and include appropriate provisions – such as processes for mutual assistance – with safeguards. There is increasing work on harmonisation of specific areas of criminal activity – such as the Council of Europe Convention on CyberCrime and various EU Directives, that the UK will have to influence and to incorporate into UK law in some form.

As part of this process, industry should contribute more directly to supporting the investigation and prosecution of e-crime, working to the same standards as, and with, law enforcement. This will require changes to current laws and regulations – although the extent of these changes is far from clear at this

---

<sup>1</sup> Defined here as “crime that requires ICT expertise during investigation”.

time.

There are many legal issues associated with the drive to reduce e-crime. Resolving these will take time, and require parliamentary time to introduce changes to law and regulations. Three key actions need to be initiated now to create a sound legal environment:

1. Much work has been done to understand how existing law needs to be updated to include the intangible world. There is an urgent need to agree on priority changes and to schedule them into the legislative process at the earliest opportunity.
2. As part of this process, the responsibilities and liabilities of those whose systems are used for, or enable investigation of, criminal activities need to be clear and understood and there needs to be an acceptable balance between intrusion and privacy. This will require that existing laws and regulations be re-visited.
3. International jurisdiction issues being addressed by government need to be supported by those in industry with appropriate knowledge and experience to ensure any agreements are technically neutral, practical and cost-effective to implement.

## **The Way Forward**

There are four key areas where progress needs to be made to create a legal and regulatory framework that addresses the emerging digital world and the e-crime that is growing with it.

### ***Criminal Acts against ICT Systems***

The Computer Misuse Act (CMA 1990) has been around since before the widespread use of the Internet outside academic circles and is perceived to be in need of updating. There has, for example, been significant debate as to whether the CMA in its current form can be used to prosecute those responsible for denial of service attacks. The Internet Crime Forum (ICF) Legal Sub-group has undertaken a detailed study<sup>2</sup> of the extent to which the CMA can cope with advances in technology, changing methods of misuse and EU and Council of Europe (CoE) moves to harmonise crimes against computer systems. It has concluded that only minor changes are needed to maintain its perceived and actual effectiveness. Indeed, the study reinforced the view that the CMA remains a good example of technology neutral legislation.

The Home Office is considering this and other inputs to a review of the CMA. As an illustration, two key recommendations are:

- To increase the maximum penalty under s1 CMA 1990 from 6 months to 5 years. The main aim is to provide increased police powers by virtue of making the offence arrestable and, incidentally, extraditable.
- To incorporate the broader principles included in Articles 4 & 5 of the CoE Convention on Cybercrime and similar provisions in s1 1(2)(e) of the Terrorism Act 2000 – effectively creating a new offence of interference with a computer system. There needs to be a clear *mens rea* element to exclude the activities of legitimate users (such as penetration testers).

### **Recommendation 1 - for rapid action by Home Office**

*To introduce urgently amendments to the Computer Misuse Act to underpin its perceived effectiveness as a means of combating crimes against information systems, particularly in the UK and across Europe and to reinforce the message that e-crime is being taken seriously.*

### ***Criminal Acts enabled by ICT systems***

Many conventional crimes (e.g. theft, impersonation, deception) are legally defined in ways that make prosecution in the intangible world difficult or impossible. For example, the police have reported problems in relation to fraudulent obtaining of services on the Internet, where a user simply completes a registration form and obtains the service, even though the details are incorrect. Prosecuting identity theft may also become a problem, since it is often a machine that is being given a person's identity details. Businesses have always suffered from industrial espionage and ex-employees taking customer lists, etc., with them. As a company's information assets have become more valuable and

---

<sup>2</sup> See <http://www.Internetcrymeforum.org.uk/cma-icf.pdf>

central to businesses in an electronic commerce environment, the lack of criminal sanction renders such acts more serious to business and the wider economy, yet currently only civil sanctions exist. The need is for changes to the relevant laws to make the commission of a criminal offence independent of the means - i.e. technology neutral.

The Law Commission has carried out a number of studies to identify priority areas where changes are required to specific laws and regulations that would cover the majority of common criminal offences. In 1997 it produced a consultation paper on Misuse of Trade Secrets (CP 150). It has produced a consultation paper (CP 155) and a final report (LC 276) on Fraud and Deception and, in particular, has examined carefully the possibility of an offence of deceiving a machine (cf para 8.3 in LC 276). Introducing the changes recommended in these reports would significantly increase confidence in electronic business and enable a wider range of computer-enabled criminal activities to be successfully prosecuted and punished. Government needs to address implementation of these recommendations as a matter of urgency. The Law Commission also needs to review work done to date, identifying priority areas where further work is needed.

## **Recommendation 2 - for rapid action by Government**

*Initiate early and open consultation on the Law Commission recommendations for priority action and implement those agreed to be of highest importance as a matter of urgency.*

There are other issues relating to the law as it currently stands that need to be considered urgently and changes implemented where priority action is identified. Examples include:

- How can malicious hackers and the writing and/or distribution of malicious code or tools be made an offence without criminalizing the legitimate development and use of tools for system management and security testing? Article 6 of the Council of Europe Convention on Cybercrime needs careful interpretation into UK law if such pitfalls are to be avoided.
- Debate continues on issues raised by s48 of the new Sexual Offences Bill. To encourage the reporting of illegal images (especially relating to paedophilia) a practical approach is needed that doesn't expose to possible criminal prosecution for "making" not just those concerned with the legal system (law enforcement, defence lawyers, etc), but also large numbers of "civilians" (e.g. system administrators, internal investigators, support staff) who come across possible criminal activity (e.g. paedophilia) and want to record/preserve the evidence for passing to law enforcement.
- There are active debates on how spam can be controlled, with government proposals for legal remedies. It is not clear whether these will be effective.
- There continue to be debates on the interpretation of aspects of the RIP Act and Part 11 of the ATCS Act – particularly around the difference between traffic/communications data and content (which is often difficult to separate). As more experience is gained on the way these Acts work, there will be need for further clarification and, no doubt, changes to the Acts. One area under discussion is the need to remove legacy powers that enable agencies and departments to access communications data without using the RIP Act processes. There is also a view that there should not be a distinction between public and private communications providers, with the same laws and restrictions applying to both.
- There continue to be examples of badly implemented legislation. A recent example is the way the EU E-Commerce Directive has been incorporated into English law where Regulation 3(2) states that the Regulations shall not apply to any future legislation or future Statutory Instruments raised against existing legislation. This means that Regulation 17 onwards, which provides protection for ISPs against damages, criminal action, etc relating to content they might carry, don't apply to future legislation or SIs. As a consequence, an SI explicitly containing an exception for Regulation 17 onwards needs to be included in all relevant future legislation. A recent example is the Tobacco Advertising Act which makes it illegal to transmit tobacco advertising – which requires an SI to exempt ISPs under Regulation 17 onwards. As a result the ISP community now has to scan every new piece of legislation to see if a special SI needs to be introduced to maintain the exemptions allowed by Regulation 17 onwards and government departments need to raise an SI where one is needed – wasting significant effort on all sides.
- Identity cloning and forgery. It has been alleged that several million US citizens have been victims and there were nearly a thousand victims in one recently reported UK case where the

initial access was to a computer file holding data on credit card transactions. Where an individual or organisation is a victim of identity cloning, it is currently costly and time-consuming to rectify the actions of the clone and to re-establish the true identity of the victim.<sup>3</sup> Changes to the law to make it an offence to possess a cloned or forged identity are being considered, and this is an encouraging first step. This issue is already becoming a major issue of public debate. Recent government proposals for national identity cards will increase awareness of this issue.

- There are major issues associated with IPR, copyright and design rights as applied in the intangible world. Much of the current activity on the legal and regulatory front is being driven by the narrow interests of the entertainment and music industries. There are, however, wider issues of protection of commercial information and knowledge that are not as yet properly addressed. Equally, there are legitimate issues relating to fair use and personal use that need to be catered for.
- There are also conflicting rules about disclosure of evidence under certain circumstances that are currently being debated by the Digital Evidence Group (a Home Office chaired working group which aims to contribute to the development and delivery of high quality forensic recovery and examination of digital evidence and to examine the impact of this on disclosure in the context of the Criminal Justice Bill and wider work on disclosure). This may result in the need for changes to laws or regulations.

### **Recommendation 3 - for action by Government**

*That EURIM facilitate discussions between relevant government departments and agencies and key industry and professional bodies on the broader range of legal issues that need to be addressed, agreeing on the priority for those requiring urgent action.*

### **Law Enforcement and International Aspects**

There are specific areas where resolution of issues associated with e-crime cannot be solely a UK matter as many of the problems relate to the global nature of the Internet and the digital world. Some of the areas mentioned above, including identity cloning and paedophilia, are already very much international problems requiring common approaches and action across many jurisdictions. The EU Commission has already introduced Directives in some areas that attempt, not wholly satisfactorily, to address some of these international issues. In particular the EU seeks to harmonise member country's treatment of crimes against ICT systems – covered in the UK by the CMA 1990.

A major need is for more effective co-operation across jurisdictional boundaries. The harmonisation (EU speak *approximation*) of penalties with regard to specific computer-related crimes such as denial of service and hacking across EU member states, the Commonwealth, the Council of Europe and other international groups may help but is only a small part of the problem. Significant harmonisation of criminal law and legal processes across Europe (let alone internationally) is unlikely in the foreseeable future for cultural, social and constitutional reasons. Cross-border investigations can, however, be greatly facilitated by the G8 24/7 contact process and effective mutual assistance arrangements. Organisations that operate internationally are often faced with particular problems where key parts of their operations (such as server systems) are installed outside the UK but UK law requires access to them. There is an urgent need to make it easier for such organisations to report and investigate suspicious incidents, and to provide information to help investigations in the UK without facing legal sanctions or complex processes.

The immediate need is to facilitate low overhead co-operation at the start of the investigation when the location of those causing the problem (which may not yet have been identified as unequivocally criminal) it is still unclear. Government must work with industry in ensuring that those with front-line experience and responsibility contribute directly to the debate in international forums and to the development of practical solutions, and that there is the continuity of representation necessary to secure action.

This will require funding if the voices of small firms and victims are to be heard amidst the cacophony of special pleading by vested interests at such events. It will also require government departments to

---

<sup>3</sup> Two recent studies into identity theft/cloning can be found at <http://www.washingtonpost.com/> and <http://www.guardian.co.uk/comment/story/0,3604,1017365,00.html>

involve industry in inter-government forums discussing such issues.

#### **Recommendation 4**

*That government ensures that joint UK industry - law enforcement teams, with cross departmental support and direct experience in the issues under discussion, are active participants<sup>4</sup> in those forums which discuss global co-operation in the fight against e-crime. This must include early and continuous industry involvement in the development of proposals and legislation that is both practical and, as far as possible, technically neutral.*

#### **Industry support for Investigations**

The EURIM-IPPR paper on [Roles and Procedures for Investigations](#) recommends that industry and law enforcement work together to combat e-crime. This requires the sharing of scarce resource and of the investigation and, where appropriate, prosecution of e-crimes. The paper makes specific recommendations on how this might be achieved, including:

- Sharing of guidelines, codes of practice, standards and tools relating to the investigation of e-crime, to mutual advantage. This should apply both to UK originated information and that produced by EUROPOL and the like to facilitate international co-operation.
- Certification of industry people with particular skills and competencies as capable of working to the same standards as law enforcement in that area.
- Identification of particular criminal activities where industry might contribute more directly to supporting law enforcement in investigation and prosecution of such crimes.

These recommendations may require changes to current laws and regulations to enable them to be implemented. For example, what legal changes are needed, if any, to enable industry and others to investigate e-crimes using appropriate rules on admissibility of evidence, processes for preservation and disclosure of relevant information, the certification of suitably experienced people to work to the same standards as law enforcement, issues relating to the governance of co-operation between industry and law enforcement in combating e-crime, the extent to which industry could contribute more directly to the prosecution of specific types of criminal activity? The extent of any legal changes necessary to enable particular activities within the private sector needs to be ascertained. Once the priority areas for consideration have been decided the legal implications need to be identified and acted on. That paper also mentions the Dedicated Cheque and Plastic Card crime unit (DCPCU), a joint operation between law enforcement and the financial services industry largely staffed by industry expertise but working under a law enforcement remit, as a good example of such joint working that could be used as a model on which to build.

#### **Recommendation 5**

*That government work with appropriate UK industry and law enforcement bodies to discuss the legal implications of recommendations that result from the work on encouraging joint activity on the investigation and prosecution of e-crime, identifying priority actions for urgent implementation – particularly those that require changes to law or regulation.*

#### **Awareness and Training**

The body of this paper focuses on changes to laws and regulations necessary to be able to counter e-crime effectively. For these changes to be effective it is also necessary for those working across the public and private sectors to be made aware of their responsibilities and obligations under various laws and regulations. This is addressed as part of the EURIM-IPPR paper on [Growing the Necessary Skills](#).

Professional bodies, training providers and those accrediting qualifications need to ensure that the relevant legal knowledge is included in appropriate training and other educational activities. There is a

---

<sup>4</sup> It is recognised that the UK cannot always choose how it is represented at international forums. However, better ways are needed of involving those with direct knowledge of the practical and business implications of topics under discussion in UK input to such forums when direct representation is not possible.

need to make such bodies aware of their responsibilities in this area. Typical areas for consideration include:

- The need for a Guide for a broad range of staff including System Administrators, Network Managers and support staff on how to handle suspected illegal material found during the course of their normal work. This will be significantly affected by the wording of s48 of the Sexual Offences Bill. It will also be affected by other legislation such as the DPA, the RIP Act, Guidelines on the handling of computer-based evidence and the like.
- Advice to those responsible for the security of information systems and networks on what tools and techniques they can use to check their security processes in what ways to avoid prosecution under malicious hacking or similar legislation.
- The need for a standard form of statement of compliance with particular laws and regulations (such as race relations, DPA), enabling companies to trust that those with whom they might be doing business electronically do conform to relevant laws.

### **Recommendation 6**

*That EURIM facilitate agreement between key private sector and professional bodies on the priorities for production of guidelines on legal issues for particular communities. This must be done consistently with parallel activities under other parts of the overall E-crime Study.*

© Copyright EURIM 2003. All Rights Reserved. For written permission to reproduce any part of this publication please contact the Administrative Secretary, EURIM, (email: admin@eurim.org; fax 01984 618383). This will normally be given provided EURIM is fully credited. Whilst EURIM has tried to ensure the accuracy of this publication, it cannot accept responsibility for any errors, omissions, mis-statements or mistakes.