All Party Parliamentary Internet Group

Chairman: - ***Derek Wyatt MP***
Joint Vice Chairmen: - ***Richard Allan MP & Michael Fabricant MP***
Treasurer: - ***Brian White MP***
Group Secretary: - ***Nick Palmer MP***

"Revision of the Computer Misuse Act": Report of an Inquiry by the All Party Internet Group

June 2004

APIG
ALL PARTY INTERNET GROUP

Revision of the Computer Misuse Act

Report of an Inquiry by the All Party Internet Group

June 2004

Introduction

1. The All Party Internet Group (APIG) exists to provide a discussion forum between new media industries and Parliamentarians for the mutual benefit of both groups. Accordingly, the group considers Internet issues as they affect society, informing current parliamentary debate through meetings, informal receptions and reports. The group is open to all Parliamentarians from both the House of Commons and the House of Lords.

2. APIG issued a Press Release (*see Appendix A*) on 16th March 2004 to announce its intention to hold an inquiry into the desirability of revising the Computer Misuse Act 1990 (CMA), and in particular:

> "whether the CMA is broad enough to cover the criminality encountered today; whether the CMA's generic definitions of computers and data have stood the test of time; whether there are "loopholes" in the Act that need to be plugged; what revisions may be needed to meet our international treaty obligations; and, whether the level of penalties within the CMA is sufficient to deter today's criminals"

3. Written submissions to the inquiry were received from:

Association for Payment Clearing Services (APACS)
Association of Remote Gambling Operators (ARGO)
Mike Barwise, Computer Security Awareness
Fiona Branson
British Computer Society (BCS)
BT Group
Lord Justice Buxton
Ron Compton
Confederation of British Industry (CBI)
Francisco De Freitas
Energis
EURIM
Clive Gringras, Olswang
Mark Hackett
Phil Hards, Computer Crime Consultants
Home Office
Independent Committee for the Supervision of Standards of Telephone Information Services (ICSTIS)

Information Assurance Advisory Council (IAAC)
inMezzo Technology Ltd
Institution of Electrical Engineers (IEE)
Internet Awareness and Advisory Foundation (IAAF)
Internet Service Providers Association (ISPA UK)
Simon Janes, Ibas
R F Kearns
Richard Kelsall, Millstream Software
David Kelsey
Barry J Mathias
Microsoft Ltd
Robert Paley, Lever Technology Group plc
Andy Pepperdine
Chris Pounder
Prevx Ltd
Real Time Club
Peter Sommer
Brian Tompsett
UKERNA
Richard Wendland, Codeburst Ltd

4. On the 29th April 2004, the committee heard oral evidence in public from:

Edward Andrewes, Committee Member, ARGO

Jeremy Beale, Head of e-Business Group, CBI

Bruno Brunskill, Board Member, IAAC

Andrew Cormack, Chief Security Adviser, UKERNA

Jim Cottrell, Head of Security Management, Energis plc

Leslie Fraser, Security Development Consultant, BCS

Clive Gringras, Partner, Olswang & Chair ISPA Legal Forum

Simon Janes, UK Managing Director, Ibas Ltd

Kevin McNulty, Policy Adviser, Hi Tech Crime Team, Home Office

Tom Mullen, Manager, Detective Operations, BT

Andrew Pinder, e-Envoy

Nick Ray, Chief Executive Officer, Prevx Ltd

Mike Rodd, Director of External Relations, BCS

Marc Sunner, Chief Technical Officer, MessageLabs

Colin Whittaker, Head of Security, APACS

Tim Wright, Head of Hi Tech Crime Team, Home Office

5. We are grateful for all the written and oral evidence that we received and also for the expert advice and assistance afforded by our specialist adviser, Richard Clayton of the Computer Laboratory, University of Cambridge.

Structure of this report

This report starts by considering the historical background to the Computer Misuse Act 1990 (CMA) and briefly describes the current statute.

We then consider the issue of definitions and whether the Act is sufficiently broad to cover the systems that it should. We move on to consider the suggestions that have been made to us as to how the CMA should be extended. This is the most substantial part of our report and we group these suggestions together by topic, specifically considering Fraud, Unauthorised Access, Security, Spyware and Denial-of-Service.

We consider the various international initiatives that will set requirements for the law in the UK. We then consider the penalties available under the CMA to determine if they need changing. We discuss the evidence presented to us on the way that CMA offences are investigated and brought to court and consider the issue of private prosecutions. The report finishes with a brief look at a few issues that do not neatly fit anywhere else and a summary of the recommendations that we have made.

A glossary is provided *in Appendix B* for those unfamiliar with the technical terms and abbreviations that are used throughout the report.

Finally, *in Appendix C*, we provide a short bibliography of relevant documents that can be consulted for further and more detailed information about the issues we discuss.

Background

6. Criminal activity involving computers has a long history and in the 1980's a number of existing statutes were used in prosecutions, such as criminal damage (Cox v Riley, 1985; R v Whiteley, 1991) and fraud (R v Lamberti and Filinski, 1987).

7. Eventually, existing legislation proved to be inadequate to cover all of the activities involved in 'computer hacking'. In particular, Robert Schifreen and Steve Gold were initially convicted of a number of offences under the Forgery and Counterfeiting Act 1981 after they had used passwords without permission to obtain unauthorised access to electronic mailboxes on the Prestel system. However, on 21st April 1988 the House of Lords overturned their convictions, agreeing with Lord Lane C.J. in the Court of Appeal that there had been a "Procrustean attempt to force the facts of the present case into the language of an Act not designed to fit them".

8. Events then moved, for legislative matters, extremely rapidly. In September 1988 the Law Commission published a consultative document on 'Computer Misuse'. In April 1989 Emma Nicholson MP introduced a private members bill to make various hacking activities illegal, but this was widely perceived to contain a number of faults and failed through lack of time. In October 1989 the Law Commission published its final report on Computer Misuse (#186) which recommended the three offences we have today. The actual legislation to implement them was brought forward as a private members bill by Michael Colvin MP. This Computer Misuse Bill received its second reading in the Commons on 2nd May 1990 and was given Royal Assent on the 29th June 1990.

9. The Computer Misuse Act 1990 deals with just two mischiefs. In s1 it criminalises "unauthorised access to computer material" and in s3 "unauthorised modification of computer material". The offence in s2 is a more serious version of s1 where there is an intent to commit or facilitate further offences.

10. The CMA claims considerable jurisdiction in that offences are committed if the person committing them is within the UK or if the computer that is affected is within the UK. The exact tests to be met differ subtly between the three offences and there are complications relating to events that take place in more than one of the home countries. The general point remains however, that there is scope for prosecuting those within the UK who attack foreign machines and those abroad who attack UK machines.

11. The CMA also contains a provision for search warrants to be issued for s1 offences (necessary because the offence is more minor than that in s2 and s3) and sets out time limits for the bringing of charges. We received no evidence suggesting these time limits need to be altered.

The Definition of Computer

12. The CMA does not contain a definition of "program", "data" or indeed "computer". This was entirely intentional, and as recommended by the Law Commission, because this approach permits the courts to determine whether a particular set of facts falls within the ambit of the Act and thereby ensures that as technology advances there is no need to amend outmoded definitions.

13. Attempts were made to add definitions during the progress of the legislation through Parliament, but these were not successful. The concern then was that the Act might turn out to cover too many devices, whereas the concern expressed to us now by several organisations is that it covers too few. To pick out just a couple of examples, the IAAC wanted to cover "mobile devices", "personal digital assistants" and "palmtops" and Energis wished to cover "network devices" such as routers.

14. Our attention was drawn to the 'Convention on Cybercrime' which uses the term "computer system". It defines a computer as a device that runs a "program" to process "data" but does not define these other terms. We were also asked to examine the 'EU Council Framework Decision on attacks against information systems' because it uses the term "information system" which is specifically intended to include networks as well as the devices which they connect.

15. However, we were also presented with extensive evidence that there had been no difficulties with the (lack of) definition of any of words in the CMA. The Home Office told us that they had "never come across a case" where the courts had failed to use a "broad definition". Peter Sommer, who has considerable experience of CMA cases as an expert witness, told us that as far as the definition of computer was concerned he was "not aware that this has caused any difficulties". Clive Gringras stressed the advantages of being able to move with the times rather than fixing upon a single notion and specifically drew our attention to the obvious presence of computers running programs within devices such as mobile phones or routers.

16. During the oral evidence session we made a particular point of enquiring after actual examples where the lack of explicit definition had been a problem and no-one was able to provide any such example.

17. From all of this we conclude that the current arrangement whereby key words are not defined within the Act is working perfectly adequately. **We recommend that the Government resist calls for words such as "computer" to be defined on the face of the Computer Misuse Act and continue with the scheme whereby they will be understood by the courts to have the appropriate contemporary meaning.**

18. Microsoft specifically requested that the definitions within the CMA be extended to include Digital Rights Management systems (DRMs) where the system might be overcome by access to data by an end-user on the end-user's own system and so

authorisation, in its normal sense, would not be at issue. We note that conditional access systems ('Pay TV'), a related set of technologies, already have their own specific legislation at EU level and also in the UK. We also observe that there has recently been a lively debate on 'Technical Protection Measures' in the context of the Intellectual Property Rights Enforcement Directive.

19. We do not consider it appropriate to attempt to shoehorn the, rather different, issue of legal protection of DRM systems into the confines of the CMA. However, **we recommend that the Government move promptly to set out proposals for a legal framework for Digital Rights Management Systems (DRMs) in a consultation document upon this important topic.**

Extending the Scope of the Act

20. Many respondents called on us to widen the Act to deal with further offences that involve computers. We were regularly informed that the world was different now than it was in 1990 when the Act was passed and therefore the CMA had passed its "sell by" date and it was important to address the new criminality that was now occurring. We discuss the various categories of extension below.

21. However, before doing so, we wish to observe that the world is not as different in 2004 from 1990 as some people seem to believe. To take just one example from many, we were warned of new threats from widespread infection of Internet machines by widely spreading 'worms'. However, in an event that was widely reported at the time, and would have been known to parliamentarians who debated the current legislation, Robert T. Morris, a Cornell graduate student, let loose a worm on the then ARPANET in November 1988. He was convicted under the US Fraud and Abuse Act and sentenced to three years of probation, 400 hours of community service and a $10,500 fine.

22. Also, the CMA is not as ineffective and tightly drawn as some other respondents seem to believe. We were asked to extend it to deal with "hacking" – quite clearly already covered under s1 – and "distributing viruses", which is covered in s3 and has been used to send several virus writers to jail, with the first case being in 1995.

23. Since these misapprehensions occurred in the evidence presented to us by people with a special interest in the topic, we can only conclude that there must be widespread ignorance of the current law and what types of activity its provisions already address. This is an entirely undesirable state of affairs.

24. Definitive legal advice must of necessity be obtained from professional lawyers, but there is an obvious need for accurate, updated, material that provides clear English explanations of legislation to the general public. The Home Office website already contains explanatory material about recent statutes, for example the Regulation of Investigatory Powers Act 2000, and this material can be linked to by ISPs and others who wish to have something more accessible than the words of the Act to refer to.

25. The Home Office has responsibility for a significant amount of legislation so that it will be taking them some time to document all of the backlog. However, we believe that it is important to prioritise the provision of website material about the CMA because it is directly relevant to Internet users and because it is clearly widely misunderstood.

26. Accordingly, **we recommend that the Home Office provide educational material on their website, as they have with more recent legislation, which explains the scope of the Computer Misuse Act and the effect of the now substantial case law. This will provide a valuable resource for others to link to, will reassure the public, and will perhaps even discourage potential miscreants.**

27. We also received a short, but extremely pertinent, response from Lord Justice Buxton. He put it to us that parliamentary time was unlikely to be forthcoming for any amending legislation unless we could point to actual cases where:

    - conduct has occurred which should be legitimately controlled by the criminal law;
    - sufficient evidence of that conduct was available;
    - the 1990 Act did not permit a prosecution to be brought.

    We have considered all the suggestions made to us in the light of these tests, which we consider to be soundly based, and this has meant that we have made considerably fewer recommendations for change than were urged upon us.

Extensions: Fraud

28. ICSTIS drew our attention to issues with premium rate diallers. These disconnect a standard dial-up connection to the Internet, and make a call to a premium rate number that permits access to specialised content. ICSTIS regulate these programs, requiring, for example, an on-screen indication of expenditure and automatic disconnection once £20 has been spent. ICSTIS told us that some diallers connect even when the user selects "cancel" and some users were getting bills of more than £500 – which they found impossible to associate with any identifiable site making legitimate use of a premium rate dialler. ICSTIS wanted more clarity on what the CMA treated as fraud.

29. In some of the circumstances that ICSTIS described we feel certain that existing legislation, but not necessarily the CMA, is sufficiently widely cast to permit criminal prosecution. **We recommend that ICSTIS proceed with criminal prosecutions of those who profit from fraudulent premium rate diallers.**

30. APACS drew attention to the huge rise in "phishing" attacks where users were conned into visiting fake web sites and disclosing security credentials. If these credentials were used then clearly a crime was committed, but APACS wished to see the tools and techniques criminalised. However, since these were 'dual-use' and there would be difficulty in distinguishing legitimate usage of these tools, they suggested an offence of possession of security credentials without a legitimate excuse.

31. The Theft Act 1978 (as amended by the Theft Amendment Act (1996) describes "obtaining services by deception" in terms of what one person may do to another. There is case law holding that this does not apply to "deceiving a machine". Hence, as several people pointed out to us, "theft of service" may not always be an offence if an automated system has been misled. The Law Commission reported on this topic in July 2002 (Report #276) proposing a Fraud Bill that addressed exactly this issue.

32. Several respondents mentioned "theft of data" to us, observing that it is not appropriate to prosecute this under the Theft Act because there is no permanent deprivation from the owner. Simon Janes told us that stolen customer databases had almost become a commodity to be traded in the marketplace. However, as Clive Gringras pointed out, where the data is on a computer then a CMA s1 offence is committed by accessing it. Peter Sommer drew our attention to the Law Commission Consultation Paper (#150) on Misuse of Trade Secrets which also addresses this area. The Law Commission have yet to produce a final report on this topic.

33. We are concerned about the current loophole concerning "deceiving a machine". We believe that there is much merit in the Law Commission's draft Bill that deals very effectively with this issue. In addition, their proposed offence of "false representation" will squarely address "phishing". The wording of the Bill would also assist ICSTIS in simplifying what they must prove to be sure of success in all prosecutions of fraudulent premium rate diallers. We do not accept the arguments put to us that all these issues

should be addressed in a revision of the Computer Misuse Act, but we do believe that legislation is required.

34. During the period that we were creating this report the Government finally announced a consultation on Fraud Law Reform, very much along the lines of the Law Commission recommendations of two years ago. We will be submitting a copy of this present report to the officials in the Home Office who are conducting the consultation to ensure they are aware of the issues that have been raised with us.

35. We welcome the Home Office consultation since this is a clear sign that the Government are finally intending to take action for reform the law on fraud. **We recommend that the Government avoids any further unnecessary delay and, once they have digested the responses to their consultation, they move swiftly to bring a new Fraud Bill before Parliament.**

36. **We also recommend 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'.**

Extensions: Unauthorised Access

37. One of elements of the s1 offence is that access to the computer is known to be unauthorised. This causes problems when some access is permitted and some is not. In *R v Bignell 1997* access to data held on the Police National Computer (about who was parked outside an ex-wife's house) was held not to be unlawful under s1 of the CMA because the police officers involved were authorised to access the system. However, in an extradition case, *R v Bow Street Magistrates Court and Allison: Ex Parte Government of the United States 1999*, the House of Lords held that although there was an entitlement to access some information about credit cards on a computer system, there was not authorisation to access the relevant information, which was subsequently used in the theft of $1million from US cash machines.

38. Several respondents drew our attention to potential difficulties that remained in this area. Microsoft thought that a tightening up of the wording might assist in prosecuting the senders of 'spam' who use email facilities provided for a legitimate purpose for another, entirely unacceptable, activity.

39. Peter Sommer pointed out that websites implicitly authorise access to their contents, but some of the data they hold is not for general usage. In *R v Raphael Gray 2001*, a teenage 'hacker' pleaded guilty to stealing credit card details from e-commerce websites by the simple expedient of invoking insecure access methods that were installed by default and incompetent webmasters had not removed. The accused pleaded guilty, so that the possible defence – this was not unauthorised access because there was nothing special about authorised access – was not tested.

40. We accept that some legal opinion believes that there are arguable issues here, but we have not been convinced that there are practical problems at the current time. The *Allison* case, decided at the highest level, goes into considerable detail on the notion of authorisation and goes to some pains to discuss the issues that arose in *Bignell* and to override some of that judgment. Excepting the unlikely event that some new case created a substantial loophole, we can see no pressing need for change.

Extensions: Security

41. A number of respondents argued that there were two sides to computer misuse and that offences for those who attacked computers should be balanced by considering offences for those who failed to secure them properly and thereby put data, or the community as a whole, at risk.

42. Richard Wendland provided an example of a poorly managed secondary school system with no effective procedures for applying security patches or auditing access control settings. There was no effective security to prevent pupils from encountering confidential letters and examination marks. When the school discovered that pupils had been accessing this material they decided they had been "hacked", excluded six pupils and considered calling in the police.

43. The Data Protection Act 1998 requires data controllers to adhere to eight principles. Principle #7 requires "appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss of, or damage to, personal data". However, not all data on computers is personal data so this is not a general requirement for security measures.

44. Firewalls are often touted as a magic cure-all for security problems. We were asked to consider everything from an education campaign about their benefits to making it a criminal offence for ISPs to fail to supply a firewall when you bought a connection to the Internet. Firewalls are often an important component in the creation of a secure environment, but for end-user systems they sometimes turn out to be an expensive way of obtaining a false illusion of security.

45. Many insecurities arise from systemic problems with computer software rather than from computer owners recklessly misconfiguring their machines. Considerable efforts are being made by software vendors, and by industry generally, to improve system security and to ensure that security problems are rapidly patched. We see no real benefit from introducing criminal offences into what is already a complex technical area.

46. Microsoft wanted an exception made to the s3 CMA offence of unauthorised alteration of data where the change was made by a software supplier and the change was done on the basis of informed consent, albeit on an "opt-out" basis. Since software companies form a contract with their customers we are unable to understand why this issue cannot be addressed within that contract. We do not agree that software suppliers should be given carte blanche to alter end-user systems without consent.

47. BT asked us to consider revising the CMA to address the extent to which a system owner can take "active measures" to secure their system without committing an offence. They clearly envisage situations where they 'scan' their customers for security holes or make a reverse connection as a check before granting access to an incoming requestor. We do not see a need for revision here since ISPs can address these matters via contract with their own customers. They can then perform scanning actions, provided that they are of a form that might reasonably be expected, by relying on the notion of authorisation that *Allison* sets out.

48. It is clear that many Internet users are, entirely unintentionally, operating insecure systems and therefore we see considerable benefits from proactive scanning for vulnerabilities by ISPs – so that customers can be assisted in correcting the problem. Industry should have common guidance as to how this scanning should be performed in a lawful manner. We repeat our recommendation from paragraph #72 of our recent report on 'spam' (see Appendix C for details): **We recommend that the ISP industry develop Best Practice procedures for proactive monitoring of the security of their customers' machines.**

Extensions: Spyware

49. A number of respondents drew our attention to 'spyware'. This term was used in a very generic way, and covered a number of different types of behaviour. This included software that will regularly 'pop-up' extra browser windows, containing advertising, as the user browses the web as well as software that can communicate usage information to remote systems without the knowledge of the computer owner.

50. Many popular programs are bundled along with 'adware', with sales of the advertisements funding the provision of the program. Legitimate operations will make the connection clear, leaving the user to make their own trade-off between the costs and benefits of using the program. However, it is not uncommon for the existence of the adware to be buried within the, seldom read, end-user licence agreement – and if the software becomes a nuisance it may prove to hard to remove effectively.

51. Other programs surreptitiously 'report home' about user browsing habits and may also extract identity information that the user has provided to other programs. There is a range of legality here, though it is quite unusual for such programs to take steps to ensure 'informed consent' to their installation.

52. There is also a range of obviously illegal activity, from unwanted redirection of browser home pages, through keyboard loggers that can steal passwords, to the premium rate diallers we have already discussed above.

53. We note that the CMA s3 offence of unauthorised addition or alteration of computer data already addresses the most egregious behaviour. We do not believe that extending the CMA to cover adware would be the right approach. Instead, we would suggest that in most instances the harm will already be addressed by the provisions of the Data Protection Act (legislation that may be unfamiliar to the US authors of these programs).

54. At the more legitimate end of the spyware market, the programs seek the permission of the user before installing themselves and thereby avoid any criminal acts. However, it is also obvious that many users have either configured their systems to automatically grant permission or have failed to understand the implications of the permission that they have granted.

55. There is an obvious rôle here for OFCOM in dealing with this 'uninformed consent' because they are charged with protecting the citizen-consumer in the digital age. **We recommend that OFCOM investigate 'spyware' with a view to developing educational material for end-users to improve their appreciation of the dangers alongside Codes of Practice for software companies that ensure they do not expose end-users to unnecessary risks. We further recommend that OFCOM works with the Department of Trade and Industry to ensure that consumer protection legislation is robust enough to ensure that contracts are clear and understandable within the online world.**

Extensions: Denial-of-Service Attacks

56. A Denial-of-Service (DoS) attack occurs when a deliberate attempt is made to stop a machine from performing its usual activities by having another computer create large amounts of specious traffic. The traffic may be valid requests made in an overwhelming volume or specially crafted protocol fragments that cause the serving machine to tie up significant resources to no useful purpose. In a Distributed Denial-of-Service (DDoS) attack a large number of remote computers are orchestrated into attacking a target at the same time.

57. In some cases the attacks overwhelm the connecting links to a machine rather than the machine itself. Clearly this can result in significant collateral damage that extends beyond the machine that is actually being attacked.

58. DoS and DDoS attacks are extremely common on today's Internet with academic studies measuring over 4,000 a week. There are many different types of attack and the volume of traffic involved varies hugely, so it is difficult to generalise about their impact. At the lower end of effectiveness, the blips in traffic are hardly noticeable, however, at the upper end we were told of examples where large University networks were made unusable for hours at a time. Providing protection against some types of

DoS (and especially DDoS) attacks can be extremely technically challenging. It is often the case that it is very hard to distinguish legitimate from illegitimate activity and this means that genuine traffic can be discarded by protective measures.

59. We received written and oral evidence from ARGO about the criminal DDoS attacks that are currently being made on gambling websites both in the UK and elsewhere. These attacks are accompanied by monetary demands (for amounts between $10,000 and $40,000) to make the attacks stop. ARGO told us that their members would not give in to this blackmail, but that the impact on the gambling businesses had been very severe indeed. The National Hi-Tech Crime Unit (NHTCU) has become involved in the investigation, but the perpetrators are believed to be based abroad, which sets some limits upon what they are able to quickly achieve.

60. Almost every respondent from industry told us that the CMA is not adequate for dealing with DoS and DDoS attacks, though very few gave any detailed analysis of why they believed this to be so. We understand that this widespread opinion is based on some 2002 advice by the Crown Prosecution Service (CPS) that s3 might not stretch to including all DoS activity. Energis and ISPA told us that they knew of DoS attacks that were not investigated because "no crime could be framed".

61. In contrast the Government, many academic lawyers and also, we understand, the NHTCU, believe that s3 is sufficiently broad to cover DoS attacks. In April 2003 the Internet Crime Forum (ICF) Legal Subgroup pointed out that s3 did not require unauthorised access, merely unauthorised "modification of the contents of any computer". They expressed the opinion that the test applied would be whether the attack had rendered unreliable the data stored on a computer or impaired its operation.

62. Although at the time of the ICF report there had been no prosecutions for a DoS attack, this has now changed. In his oral evidence, Clive Gringras drew our attention to the recent case of *R v Caffrey* in which it was alleged that Aaron Caffrey had caused a denial-of-service attack on systems at the Port of Houston, Texas. In the event, the jury did not convict Mr. Caffrey, apparently because they did not believe him to have been responsible for the attacks. It is important to note that there does not seem to have been any attempt by the defence to have the case thrown out because the denial-of-service activity was not covered by the CMA.

63. Some respondents addressed the 'Computer Misuse Amendment Bill' proposed by the Earl of Northesk because this had attempted to bring DoS attacks squarely within the ambit of the CMA. The Bill was given a second reading in the House of Lords on 20th June 2002, but made no further progress. In the evidence we received, there was support for the aims of the Bill, but criticism of the wording, in that it had too wide a scope and set too much store on the notion of 'ownership' of systems. The general tenor of the remarks made to us was that it had been pretty much a Good Thing.

64. Other respondents suggested that DoS attacks should be dealt with by adopting the approach of the 'EU Council Framework Decision on attacks against information systems'. This explicitly sets out that a criminal offence must be committed by "suppressing or rendering inaccessible computer data", if this is done "without right".

65. We suggest that the reason for this wide disparity of legal opinion, and distrust of the efficacy of the current law, is that when DoS and DDoS attacks occur on the Internet then it is the particular circumstances of each attack that makes it obvious whether the CMA wording applies. In general, where a DDoS attack takes place then an offence will have been committed because many machines will have been taken over by the attacker and special software installed to implement the attack. Even when a system is attacked by a single machine, an offence will sometime be committed because the contents of the system will be altered. However, when the sole effect of an attack is to

fill a nearby link with useless traffic, then it may be hard to show the elements of a CMA offence are present, although a DoS attack has certainly occurred.

66. It is clearly undesirable to have the illegality of an attack depend upon the exact mechanism used so we are minded to recommend the creation of a new offence of 'impairing access to data'.

67. However, we foresee some difficulties in framing such an offence when examining notions of intent or, as the 2002 Northesk Bill proposed by its 'reasonable person' wording, recklessness.

68. We are conscious that denial-of-service can also occur through 'flash crowds' when too many people access the same site for it to cope with. An example of this would be the initial collapse of the website holding details of the 1901 census. We are also familiar with similar flash crowds on telephone networks, such as occurred when a million callers an hour tried to buy tickets for the Euro 2000 football tournament.

69. These flash crowds may have an obvious single cause. Are we to lay a broadcaster open to prosecution if they mention a website on the air and several million people suddenly decide to have a look at it? Broadcasters have guidelines on instigating telephone traffic and may become subject to similar guidelines for Internet material. Should we regard reckless disregard of these guidelines as a matter for the criminal law?

70. We are also aware of a growth in 'cyber-protest' whereby it is arranged for supporters of a cause to all access a web-site at the same time – with the aim of ensuring that it becomes unavailable for a short period. Where such protesters are simply fetching web pages using standard browsers we can see significant dangers in creating a framework for criminalising their behaviour.

71. Where DoS attacks are linked to more serious crime then there is already an expectation that the police will investigate and there will be scope for laying serious criminal charges. The ARGO evidence makes it clear that this expectation is being fulfilled. However, it is also obvious that the police do not have the resources to tackle even a small fraction of the DoS attacks that take place every day, and where these attacks take place across jurisdictional boundaries there may be significant barriers to their investigations. We observe that there may be negative value in creating an offence where everyone knows that, absent links with more serious criminal activity, the chances of investigation and prosecution are essentially nil.

72. Clearly the victim of a substantial DoS attack is motivated to investigate and may be in a position to know who is likely to be behind the attack. They are just as likely to be disappointed if the police review their resource constraints and do not consider it sufficiently serious to tackle as they are today when, apparently, the CPS has suggested that no offence has been committed. In such circumstances – where the DoS attack is not linked with other criminal behaviour – we can see an argument for addressing the problem via a civil case where one can seek damages and serve injunctions, rather than treating the attack as a criminal matter.

73. We now draw the main arguments together. In this section we have considered the pros and cons of revising the CMA to more squarely address the issue of DoS and DDoS attacks. We must balance the desire for the clarity a new offence would bring against the fears it will be too broad and the suspicion that if this is the only offence committed, then the police will not prioritise its investigation.

74. We accept that the CMA already makes many denial-of-service attacks illegal, but we believe that there would be very significant value in adding an explicit offence to the legislation. In particular, we consider that this would send a clear message to the police, to the CPS and to the courts that these attacks should be taken seriously. In addition,

publicity about the new offence will reach DoS attackers and some will be deterred by knowing, without the doubts currently expressed, that their actions are clearly criminal.

75. We do not have a strong view as to whether a separate Bill is needed to amend the Computer Misuse Act or whether the new offence could be brought in via one of the Home Office's regular portmanteau Criminal Justice Bills. However, we do believe that there is no benefit to excessive delay, and **we recommend that the Home Office rapidly bring forward proposals to add to the Computer Misuse Act an explicit 'denial-of-service' offence of impairing access to data. The tariff should be set the same as the s1 'hacking' offence. There should be a further 'aggravated' offence along the lines of the current s2 where the denial-of-service is merely one part of a more extensive criminal activity.**

Extensions: International Obligations

76. We have already mentioned in passing two important international initiatives that address computer misuse, the 'Convention on Cybercrime' and the 'EU Council Framework Decision on attacks against information systems'. In this section we will examine more closely the extent to which they might lead to revision of UK legislation.

Cybercrime Convention

77. The 'Convention on Cybercrime' was created by the Council of Europe, in conjunction with the United States, Canada, South Africa and Japan. It currently has 37 signatures and five states (Albania, Croatia, Estonia, Hungary and Lithuania) are recorded as having ratified it. It will come into force – for the ratifying countries – on 1st July 2004. The UK is a signatory, but will be unable to formally ratify the convention until UK law is fully in compliance with the obligations it contains. The Government have previously indicated that they wish to achieve this by 2005.

78. Most of the requirements of the convention are already covered by UK legislation. We have already referred to the controversy relating to denial-of-service which the convention expresses in article 4 and 5 as the need to criminalise "suppression of computer data" though it is permissible to require that this result in "serious harm".

79. The only topic that is not currently addressed by UK law is the requirement in Article 6 to create a criminal offence, when committed "intentionally and without right" of the "production, sale, procurement for use, import, distribution or otherwise making available of […] a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing [CMA type offences]".

80. There are other possible offences that could be created in relation to Article 6, that relate to making 'hacking tools' available. However, such offences would result in significant difficulties because almost all these tools are 'dual use' and are widely employed by security professionals and system administrators. The Home Office have indicated that they are unlikely to criminalise this latter class of items, but they are addressing a similar issue in their consultation on revising Fraud legislation in relation to possession of items, such computer templates for producing utility bills, as used in 'identity theft'.

81. Peter Sommer raised some doubts about the international aspects of the Convention as it applied to evidence collection and warranting. He suggested that differing rules in other jurisdictions for disclosure of evidence to the defence might cause prosecutions to collapse in the UK. This is not a matter for the CMA but is obviously one to be addressed as multi-jurisdictional investigations become more common.

82. We received very few comments on the implications for the CMA of ratifying the Convention on Cybercrime, suggesting that this is not widely seen to be a contentious issue. We are pleased to see that the Home Office is not intending to attempt to criminalise 'hacking tools' because we believe that this will cause unnecessary confusion and anxiety for the many legitimate users of these programs. **We recommend that the Home Office maintain their current approach and continue to resist any calls to implement the 'optional' parts of Article 6 of the Convention on Cybercrime.**

EU Framework Decision

83. The 'EU Council Framework Decision on attacks against information systems' was proposed on 19th April 2002, 'political agreement' was reached on 28th February 2003 and the final text, dating from 20th June 2003, is expected to be formally adopted during the summer of 2004, shortly after this report is published. The UK will then have two years to implement measures to comply with the provisions of the Framework Decision.

84. There are a number of technical issues that arise with the Framework Decision because the legal language within it differs from that used in the UK. In particular, as we have already commented upon, it uses the notion of "information system" which extends to the network as well to the computers that the network connects. It also uses the phrase "without right" which is different from the UK concept of "authorisation" even when the *Allison* judgment is considered. **We recommend that the Home Office resist any temptation to "gold plate" European legislation, since it is reasonably clear that UK law will meet the needs of the 'Framework Decision on attacks against information systems' in spirit if not to the letter. We see little value in using parliamentary time on making changes here just for the sake of it.**

85. We received very few comments about the Framework Decision, except in so far as respondents believed that adopting its language on "information systems" would be useful. They believed that it would assist in ensuring that the definition of "computer" was as wide as they wished and the also thought that it would assist in ensuring that the CMA dealt with denial-of-service attacks. We have covered these issues elsewhere and make no further recommendations here.

Extensions: Miscellaneous

86. We received a submission from a member of the public who suffered a six-month campaign of online harassment. In the end the only offence the perpetrator was charged with was "breach of the peace". They considered that a number of other activities that formed part of the harassment, in particular masquerading as other people and diverting email, should have been pursued and they were not pursued because they were not offences. Although we have considerable sympathy for anyone who is in this sort of position, we do not accept the view that any crime relating to computers should come under the Computer Misuse Act. We also express surprise that diversion of email does not amount to an offence under the Regulation of Investigatory Powers Act 2000.

87. Many respondents mentioned unsolicited bulk email or 'spam' and Microsoft specifically wished the sending of spam via 'open relays' and 'open proxies' to be criminalised. We fail to see why unauthorised access to a machine and the relaying of traffic via its systems is not already covered by the CMA. We have, however, produced a previous report on the topic of 'spam' (see Appendix C) and we will not repeat its conclusions and recommendations here.

Length of Sentences

88. At present, a summary conviction under the CMA has a maximum penalty of six months imprisonment and/or a fine of £5,000. A conviction on indictment is currently only applicable to s2 and s3 offences and there the maximum penalty is five years imprisonment and/or an unlimited fine.

89. These are, however, maximum sentences. Home Office figures show that where a CMA offence is the principal offence with which someone is charged then only about one third of those found guilty are given a custodial sentence. Where the CMA offence is not the principal offence it is a very small proportion indeed. We were told that it is often the case that CMA offences were 'plea bargained' and not proceeded with because justice had been done some other way.

90. Several respondents felt that the current maximum scales were about right. BT observed that s1 did not need to have a very high tariff because s2 was available to deal with cases where serious criminality was involved. They also drew attention to the significant impact of confiscation powers – seizing their computers – on the type of individual who was caught up in s1 offences. They also suggested that voluntary hand-over of computer equipment as a condition for receiving a formal caution produced a similar deterrent effect.

91. Peter Sommer observed that his experience of assisting in the defence of many people who had been accused of CMA offences had persuaded him that there was unlikely to be a significant deterrent effect to higher sentences because "many hackers occupy a fantasy world where they believe they will never be caught". UKERNA and BT also suggested that it was lack of investigation that led to a lack of deterrence rather than the length of sentence being risked. Peter Sommer put it to us that there were drawbacks to society in putting some types of offender into prison, where they would come into contact with serious and organised crime.

92. Other respondents drew our attention to the very significant damage that could be done by computer misuse. It is regularly claimed that the cost of cleaning up after virus and worm attacks runs into billions of dollars. They believed that the current level of sentences did not properly reflect the seriousness of the offences. The attack on the Port of Houston in the *Caffrey* case was widely viewed as an attack on the US 'Critical National Infrastructure' and this should be treated accordingly gravely.

93. A common suggestion was that longer sentences should be imposed for s1 because of the side effects this would have. Raising the tariff to one year would make the offence extraditable. Making s1 indictable would make it possible to prosecute for a criminal attempt at the offence, viz: it would not have to actually succeed. Raising the tariff to five years, in line with the s2 and s3 offences, would make the s1 offence 'arrestable' and this would also mean that search warrants were more easily obtained by using the PACE 1984 provisions.

94. Early drafts of the EU Framework Decision required the maximum sentence for the s1 offence to be raised to at least one year. Although this has now been removed from the text, the discussions caused the Home Office to consult with law enforcement agencies and the CPS to review the s1 penalty. In particular, they considered the details of cases where someone was charged with a s1 offence, yet their actions – and the damage caused – warranted a higher sentence than six months but, for example, there was insufficient evidence to expect to obtain a s3 conviction, with its five-year maximum.

95. The review's conclusions led to Home Office Ministers agreeing to bring forward measures to raise the maximum penalty for s1 to two years. The Home Office is also

reviewing s2 and s3 to determine if their sentences are in line with equivalent offences in other legislation.

96. We have considered all these points and have a few observations to make on them. The most obvious is that one does not expect that everyone convicted would receive the maximum sentence. We have confidence that the courts will not impose custodial sentences in circumstances where this is not justified by the circumstances of the crime or the guilty individual.

97. We also reject the argument that tariffs should be set at levels that are solely chosen for the expediency of the investigatory process and that s1 should be raised to five years merely to enable the police to get a search warrant without bothering a circuit judge.

98. Having made it clear that some of the arguments are lacking in merit, we find that other arguments are compelling. We are convinced that it is important to send a clear message that society now takes 'hacking offences' rather more seriously than in 1990. Statistics [Bush/Kugel] show that computer failures lead to bankruptcy in 25% of cases and that the same fate has befallen 93% of businesses that have lost their data centre for ten days or more. Where criminals have hacked into machines and thereby risked this type of disaster, then their behaviour must be punished on an appropriate scale.

99. We therefore believe there is a strong case for raising the tariff for s1 and we are content to follow the lead of the experts consulted by the Home Office. Hence, **we recommend that the maximum sentence for a conviction of an offence under s1 of the Computer Misuse Act should be raised to two years.**

Prosecutions under the Computer Misuse Act

100. A number of respondents believed that there were significant problems with the investigation and prosecution of CMA offences.

Process Issues

101. There was a clear feeling that CMA offences were underreported. Prevx suggested that firms failed to report cybercrime because of a fear of adverse publicity and individuals failed to report attacks because of a perception that the police are powerless to deal with the problem. This led to a lack of understanding of the scope or scale of the problem.

102. We were also told that there was nowhere to report nuisances such as port scanning, virus attacks, phishing scams or advanced fee fraud emails. On the law enforcement side these were seen as generally insignificant events and the existence of on-line reporting systems would provide too many reports to be processed and an expectation of action that would be impossible to assuage.

103. Many respondents complained that the police were not giving sufficient priority to the investigation and prosecution of cybercrime. It was pointed out that cybercrime was not one of the target measures by which police performance was assessed.

104. There was an appreciation of the difficulties faced by the police in investigating CMA offences because of the international scope of the problem and the lack of CMA style legislation in other jurisdictions. However, Clive Gringras asked why there had been several computer-related extraditions from the UK to the USA, but no-one had ever been extradited to the UK to face trial in this country, even though the CMA had been specially crafted to catch foreign criminals who attacked UK machines.

105. Some industry bodies seemed to believe that CMA offences were not tackled because of the difficulty of getting a conviction. APACS suggested that CMA prosecutions were so complex that they should be tried specially, as is often proposed for Fraud cases. The

CBI suggested that criminals "are being acquitted due to a jury's lack of understanding of computer issues" and there was an "inability to secure a conviction under the current computer misuse legislation".

106. BT told us that they had identified 54 hackers in the last 18 months and "had worked with the police to a successful conclusion". However, they had not used the CMA, finding it simpler to use s42 of the Telecommunications Act 1984, "Fraudulent Use of Telecommunications System". The normal result was a caution for the miscreant where they voluntarily signed over their computer equipment. BT quoted a figure of a 40% reduction in 'port scans' over the 18-month period.

107. It is clear from the evidence presented to us that a root cause of the discontent with the CMA is that the police are failing to meet expectations in the investigation of computer crime. This is an area that has recently been addressed by the 'EURIM-IPPR E-Crime Study', which is intended to feed into the Home Office policy formulation process that will result in the publication of an e-Crime strategy later this year. **We recommend that the Home Office consider the recent EURIM recommendations within their May 2004 'Supplying the Skills for Justice' paper and ensure that policies are developed that will address the need for effective policing of computer crime.**

Private Prosecutions

108. In modern times we are used to seeing the Crown Prosecution Service handling criminal prosecutions, however s6(1) of the Prosecution of Offences Act 1985 expressly preserves the ancient right to bring a private prosecution. Some statutes do require the state to prosecute, others require that permission is granted by the Attorney General before a prosecution may start. However, most offences – and the CMA offences come into this category – may be privately prosecuted.

109. To bring a private prosecution the first step is to 'lay an information' before a magistrate who will then decide whether to issue a summons. If a summons is issued then a criminal trial will ensue. However, there are some other procedural checks on private prosecutions. Firstly, the Attorney General may enter a *nolle prosequi*, which essentially freezes the process and is generally used when the accused has some mental or physical incapacity preventing them from standing trial. Secondly, and more relevantly, the Director of Public Prosecutions (DPP) may take over a case at any stage and discontinue it, decline to offer evidence or withdraw it.

110. Where the police, who are technically just individuals, commence a case then the DPP is obliged by the 1985 Act to take it over and the Crown Prosecution Service then takes it forward as appropriate. Where it is a truly private prosecution the DPP has no obligation to act and may or may not allow the case to proceed.

111. It was suggested to us, most particularly by Clive Gringras, that there are a number of companies who would wish to explore the bringing of private prosecutions for CMA offences. The implication was that the police or prosecutors had not prioritised their cases and they wished to ensure that criminals did not escape justice through lack of resources. A further reason would be the hope of a successful prosecution serving as a deterrent to prevent future attacks. However, these companies were currently reluctant to proceed with private prosecutions because of significant doubts as to whether the DPP would permit them to proceed.

112. We have already noted the considerable problems faced by the police in evidence gathering and we do not believe that the private sector will find this any easier. However, where a strong case can be built, we do not see any overwhelming public policy reason to inhibit private prosecutions under the CMA. We do not envisage that there will be many such prosecutions but we see it as a way in which private money can assist in public policing. **We recommend that the Director of Public Prosecutions set**

out a permissive policy for private prosecutions under the Computer Misuse Act, saving his extensive powers to discontinue cases only when they are totally inappropriate or clearly vexatious.

113. Jim Cottrell suggested that it might be practical to take civil action for the costs of dealing with events such as a denial-of-service attack. He drew a comparison with the civil recovery schemes operated by supermarkets that sought to recover damages from those who were convicted of shoplifting.

114. Brian Tompsett suggested that the victims of crimes such as virus attacks, exploitation of proxies, fraudulent diallers etc. should be permitted to take legal action against the perpetrators in the small claims court. He suggested that the combined influence of many injured parties would prove a strong deterrent without consuming resources from the public purse. Our difficulty with this proposal is that in almost all the examples cited, the difficulty is not in the legal framework but in accurately determining the responsible party – the immediate 'attacker' may also be an innocent victim whose computer has been compromised without their knowledge. We cannot see that individuals will have the investigative resources to avoid a considerable waste of the court's time in chasing after the wrong people.

Miscellaneous

115. As is inevitable, some of the issues on which we received evidence, and which we agree are important, do not fit into tidy categories, nor are they specifically concerned with particular legislation. This final section of our report briefly covers these topics.

116. Peter Sommer drew our attention to the lack of procedures that many victims have for preserving evidence. Most people know that in real world crimes the police can dust for fingerprints and obtain DNA profiles. Computer forensics is less well understood, though the same principle of leaving the machine alone until the expert arrives, is a useful approach – excepting that what it means to leave a networked machine alone may be less obvious, and of course, it may be that the crime is never investigated and the evidence never required. **We recommend that computer forensic experts, within the police and private industry, should create a simple checklist that addresses the ways in which evidence can be preserved for investigators. We also recommend that the police implement suitable procedures that will act as the cyberworld equivalent of taking down the 'Police Line – Do Not Cross' tapes.**

117. A common theme running through all of our recent inquiries, into Communications Data, Spam and now this one on revising the Computer Misuse Act, is that there is a dearth of statistics. Also, impact assessments, usually expressed in billions of dollars, are almost invariably reported by organisations with a vested interest in calculating extremely high values. The current system of recording crime fails to capture information such as whether computers were involved or whether there was an Internet component to the offences. This all means that the information that is needed to make well-informed policy decisions on issues affecting computers and the Internet is absent and one is left with opinions at best and usually with just a handful of anecdotes.

118. In order to obtain these statistics then clearly we do not wish to recommend onerous form-filling exercises to use up even more police time. However, it is in the nature of statistical totals that they can be approximated by carefully designed sampling techniques. That is to say, local small-scale intensive data collection is capable of providing an excellent approximation of national totals. **We recommend that the Home Office address the lack of statistics on cybercrime by means of small-scale statistical sampling, because we believe that without good figures on the scale of cybercrime activity, policy formation is unnecessarily difficult.**

Summary of Recommendations

#17 **We recommend that the Government resist calls for words such as "computer" to be defined on the face of the Computer Misuse Act and continue with the scheme whereby they will be understood by the courts to have the appropriate contemporary meaning.**

#18 **We recommend that the Government move promptly to set out proposals for a legal framework for Digital Rights Management Systems (DRMs) in a consultation document upon this important topic.**

#26 **We recommend that the Home Office provide educational material on their website, as they have with more recent legislation, which explains the scope of the Computer Misuse Act and the effect of the now substantial case law. This will provide a valuable resource for others to link to, will reassure the public, and will perhaps even discourage potential miscreants.**

#29 **We recommend that ICSTIS proceed with criminal prosecutions of those who profit from fraudulent premium rate diallers.**

#34 **We recommend that the Government avoids any further unnecessary delay and, once they have digested the responses to their consultation, they move swiftly to bring a new Fraud Bill before Parliament.**

#36 **We recommend 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'.**

#48 **We recommend that the ISP industry develop Best Practice procedures for proactive monitoring of the security of their customers' machines.**

#55 **We recommend that OFCOM investigate 'spyware' with a view to developing educational material for end-users to improve their appreciation of the dangers alongside Codes of Practice for software companies that ensure they do not expose end-users to unnecessary risks. We further recommend that OFCOM works with the Department of Trade and Industry to ensure that consumer protection legislation is robust enough to ensure that contracts are clear and understandable within the online world.**

#75 **We recommend that the Home Office rapidly bring forward proposals to add to the Computer Misuse Act an explicit 'denial-of-service' offence of impairing access to data. The tariff should be set the same as the s1 'hacking' offence. There should be a further 'aggravated' offence along the lines of the current s2 where the denial-of-service is merely one part of a more extensive criminal activity.**

#82 **We recommend that the Home Office maintain their current approach and continue to resist any calls to implement the 'optional' parts of Article 6 of the Convention on Cybercrime.**

#84 **We recommend that the Home Office resist any temptation to "gold plate" European legislation, since it is reasonably clear that UK law will meet the needs of the 'Framework Decision on attacks against information systems' in spirit if not to the letter. We see little value in using parliamentary time on making changes here just for the sake of it.**

#99 **We recommend that the maximum sentence for a conviction of an offence under s1 of the Computer Misuse Act should be raised to two years.**

#107 **We recommend that the Home Office consider the recent EURIM recommendations within their May 2004 'Supplying the Skills for Justice' paper and ensure that policies are developed that will address the need for effective policing of computer crime.**

#112 **We recommend that the Director of Public Prosecutions set out a permissive policy for private prosecutions under the Computer Misuse Act, saving his extensive powers to discontinue cases only when they are totally inappropriate or clearly vexatious.**

#116 **We recommend that computer forensic experts, within the police and private industry, should create a simple checklist that addresses the ways in which evidence can be preserved for investigators. We also recommend that the police implement suitable procedures that will act as the cyberworld equivalent of taking down the 'Police Line – Do Not Cross' tapes.**

#118 **We recommend that the Home Office address the lack of statistics on cybercrime by means of small-scale statistical sampling, because we believe that without good figures on the scale of cybercrime activity, policy formation is unnecessarily difficult.**

Appendix A: Press Notice & Guidelines for Witnesses

16th March 2004
For immediate release

Press Release – APIG to hold public inquiry on revision of the Computer Misuse Act

The All Party Parliamentary Internet Group (APIG) is to hold a public inquiry into the desirability of revising the Computer Misuse Act 1990 (CMA).

The inquiry will particularly focus upon the following:

- Whether the CMA is broad enough to cover the criminality encountered today;
- Whether the CMA's generic definitions of computers and data have stood the test of time;
- Whether there are "loopholes" in the Act that need to be plugged;
- What revisions may be needed to meet our international treaty obligations;
- Whether the level of penalties within the CMA is sufficient to deter today's criminals;

APIG calls upon interested parties to present written evidence to the inquiry before 9th April 2004.

A public hearing will be held in the House of Commons on the 29th April 2004 when MPs will question industry, Government and the public on their suggested revisions to the CMA.

Richard Allan MP, Joint Vice-Chairman of APIG said:

"As computer networks increasingly underpin our everyday activities any disruption to them can have very serious consequences. There must be effective legislation to prosecute those who maliciously attack computer networks in the same way that we deal firmly with people who cause criminal damage to physical objects. The law in this area needs updating and we will look at how this can be done most effectively."

Brian White MP, Treasurer of APIG said:

"The CMA has stood the test of the time remarkably well. However, it was drafted before the revolutionary nature of the Internet and the World Wide Web was fully known. As more people find increasingly sophisticated ways to attack our information systems, it is important we have all the protections we need. A review of the Act is therefore timely."

Derek Wyatt MP, Chairman of APIG said:

"There is a lot of very disruptive activity on the Internet, from outright hacking and the distribution of viruses, through denial-of-service attacks on systems, and right down to the sending of spam via insecure end-user machines. Some of this is clearly illegal today, but some of it seems to fall into grey areas or is difficult to deal with across jurisdictional borders. We need to know if the law, both in the UK and elsewhere, needs strengthening to ensure that we can deter bad behaviour, and also prosecute and convict where necessary."

The Earl of Northesk, Member of APIG said:

"The Computer Misuse Act dates from 1990. Fourteen years on the technological advance and increasing sophistication of the Internet has outstripped its capacity to deal with the generality of e-crime adequately. It is now two years since I introduced my Computer Misuse (Amendment) Bill which received a generous, if somewhat lukewarm, response from the Minister concerned, Lord Bassam. If strengthening and recasting of the Computer Misuse Act was urgent then - and I believe it was - it is even more so now, especially given that Home Office Minister, Caroline Flint, identified this is a priority at the National Hi-Tech

Crime Unit's second e-Crime Congress last month. Any contribution that APIG's inquiry can make to this end is welcome."

Written evidence should be submitted to inquiry@apig.org.uk by 9th April 2004. APIG may, at its discretion, ask for oral evidence from witnesses on 29th April 2004 at the House of Commons. The inquiry's report will be published in June 2004.

Note to Editors:

Derek Wyatt MP is the Labour MP for Sittingbourne and Sheppey. He is a leading campaigner on Internet issues in Parliament.

Richard Allan MP is the Liberal Democrat IT spokesman and represents Sheffield Hallam.

Brian White MP is a leading Labour backbencher on technology issues, representing Milton Keynes North East.

The Earl of Northesk is a Conservative Peer and a leading authority on IT matters in the House of Lords. In 2002 he introduced the Computer Misuse Amendment Bill, which sought to protect computerised systems against denial-of-service attacks.

The All Party Parliamentary Internet Group exists to provide a discussion forum between new media industries and parliamentarians. Accordingly, the group considers Internet issues as they affect society, informing Parliamentary debate through meetings, informal receptions, inquiries and reports. The group is open to all members of the Houses of Parliament.

Enquiries about the work of the Committee:

Telephone: 020 7233 7322

Fax: 020 7233 7294

e-mail: inquiry@apig.org.uk

APIG CMA Inquiry: Guidelines for Witnesses

The All Party Parliamentary Internet Group announced its inquiry into the "Computer Misuse Act" on March 16th 2004. The inquiry is anxious to receive as wide a range of submissions as possible.

1. More information about APIG can be found at www.apig.org.uk
2. Documents of relevance to the inquiry include:
   - Computer Misuse Act 1990

     http://www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm
   - Computer Misuse Amendment Bill

     http://www.parliament.the-stationery-office.co.uk/pa/ld200102/ldbills/079/2002079.pdf
   - The Council of Europe Cybercrime Convention

     http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
   - EU Framework Decision on "Attacks Against Information Systems"

     http://europa.eu.int/eur-lex/en/com/pdf/2002/com2002_0173en01.pdf
3. Written submissions should be concise and address the matters raised by the inquiry concentrating on the issues with which the witness has a special interest. A typical length

would be about 1,000 words. Essential statistics or further details can be added as appendices.

4. It would be much preferred if written submissions were made in an electronic format. They should be in plain text (ASCII), PDF , .DOC or .RTF format. Submissions should be dated and include the name, address and telephone number of the person in the organization who is responsible for the submission.
5. It is at the inquiry's discretion to publish any evidence it receives. Any information that a witness would not wish to be considered for publication should be clearly marked.
6. The inquiry has asked for all written evidence to be submitted by ***9th April 2004***. The Officers of APIG following consideration of written evidence, will decide, which organisations and individuals to invite to give oral evidence in Westminster on ***29th April 2004***.

Hard copies of written evidence may be submitted to:

APIG Secretariat,
23 Palace Street,
London
SW1E 5HW

But electronic submissions (in plain ASCII, Adobe PDF or Microsoft Word .DOC or .RTF formats) are preferred and should be emailed to inquiry@apig.org.uk

Appendix B: Glossary of Terms

APACS
Association for Payment Clearing Services

APIG
All Party Internet Group, a discussion forum for Parliamentarians and the new media industries and the body responsible for this report.

ARGO
Association of Remote Gambling Operators, a new trade body for online bookmakers

ARPANET
Advanced Research Projects Agency Network, the main precursor to the Internet

BT
'British Telecom'; BT are the incumbent telco in the UK and a major ISP

CBI
Confederation of British Industry

CMA
Computer Misuse Act 1990

Convention on Cybercrime
Convention created under the auspices of the Council of Europe to create a common international criminal policy aimed at the protection of society against cybercrime.

CPS
Crown Prosecution Service

DDoS
Distributed Denial-of-Service (q.v.)

Denial-of-Service
Preventing the normal operation of a computer by bombarding it with spurious traffic.

Distributed Denial-of-Service
A DoS attack that is being made from many different locations simultaneously.

DNA
Deoxyribonucleic acid

DoS
Denial-of-Service (q.v.)

DPA
Data Protection Act 1998

DPP
Director of Public Prosecutions, one of the UK's Law Officers

DRM
Digital Rights Management System

EU
European Union

EURIM
The European Information Society Group, an all-party pan-industry "lobby" group that discusses the politics of the Information Society and E-Commerce.

firewall
A firewall is a system, either hardware or software, designed to prevent unauthorised access to or from a private network or machine.

IAAC
Information Assurance Advisory Council

ICF
Internet Crime Forum

ICSTIS
Independent Committee for the Supervision of Standards of Telephone Information Services. The regulatory body for all premium-rate telecommunications services.

ISP
Internet Service Provider

ISPA
Internet Service Providers Association UK: a 'trade body' for the UK ISP industry

NHTCU
National Hi-Tech Crime Unit

PACE
Police and Criminal Evidence Act 1984

UKERNA
Trading name of the JNT Association, which manages the operation and development of the JANET network used by UK Higher Education Institutions.

virus
A computer virus is a self-replicating program running on a computer without the authorisation of the owner. Pedantically distinguished from a worm (q.v.) because it attaches itself to another program to propagate.

worm
A network worm is a self-replicating program or virus (q.v.) that spreads from machine to machine across a network.

Appendix C: Bibliography

UK legislation

Theft Act 1978

not currently available online

Forgery and Counterfeiting Act 1981

not currently available online

Telecommunications Act 1984

http://www.communicationsbill.gov.uk/legislation/Telecommunications_Act_1984.doc

Prosecution of Offences Act 1985

Computer Misuse Act 1990

http://www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm

Theft (Amendment) Act 1996

http://www.legislation.hmso.gov.uk/acts/acts1996/1996062.htm

Data Protection Act 1998

http://www.hmso.gov.uk/acts/acts1998/19980029.htm

Law Commission of England & Wales

Report #186: Computer Misuse

not currently available online

Report #255: Consents to Prosecution

http://www.lawcom.gov.uk/files/lc255.pdf

Report #276: Fraud

http://www.lawcom.gov.uk/files/lc276.pdf

Consultation Paper #150: Legislating the Criminal Code: Misuse of Trade Secrets

http://www.lawcom.gov.uk/351.htm

International initiatives

Convention on Cybercrime

http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

Proposal for a Council Framework Decision on attacks against information systems

http://europa.eu.int/eur-lex/com/pdf/2002/com2002_0173en01.pdf (19 Apr 2002)

Council Framework Decision on attacks against information systems

http://register.consilium.eu.int/pdf/en/03/st08/st08687-re01en03.pdf (20 June 2003)

Other relevant documents

Fraud Law Reform: Consultation on proposals for legislation

http://www.homeoffice.gov.uk/docs3/fraud_law_reform.pdf

Judgments – Regina -v- Stephen William Gold, and Robert Jonathan Schifreen 1988

http://www.swarb.co.uk/c/hl/1988r_goldschifreen.html

Judgments – Regina v Bow Street Magistrates Court and Allison (A.P.) Ex Parte Government of the United States 1999

http://www.parliament.the-stationery-office.co.uk/pa/ld199899/ldjudgmt/jd990805/bow.htm

Reform of the Computer Misuse Act 1990, ICF Legal subgroup

http://www.internetcrimeforum.org.uk/cma-icf.pdf

Computer Misuse (Amendment) Bill [HL]

http://www.parliament.the-stationery-office.co.uk/pa/ld200102/ldbills/079/2002079.pdf

EURIM-IPPR E-Crime Study, Partnership Policing for the Information Society, Third Discussion Paper, 'Supplying the Skills for Justice'

http://www.eurim.org/consult/e-crime/may_04/ECS_DP3_Skills_040505_web.htm

APIG

Report of an Inquiry on 'Spam', October 2003

http://www.apig.org.uk/spam_report.pdf

Report of an Inquiry on 'Communications Data', January 2003

http://www.apig.org.uk/APIGreport.pdf

Written and oral evidence submitted to this inquiry

http://www.apig.org.uk/computer_misuse_act_inquiry.htm


APIG
ALL PARTY INTERNET GROUP