

# Legislating Against Computer Misuse: The Trials and Tribulations of the UK Computer Misuse Act 1990

by Andrew Charlesworth<sup>1</sup>

## Abstract

This article examines the ability of the courts to use the Computer Misuse Act 1990 to combat computer misuse in the UK, considering some of the reported and unreported cases before and after the Act. Issues discussed include the difficulties in gaining evidence, the attitude of the legal system towards computer misuse, the public attitude towards hackers, hacking and computer crime and the use of the 'addiction defence' in the case of *R. v Bedworth and others*<sup>2</sup> and how each of these factors plays a part in making the Computer Misuse Act 1990 a much less effective tool in combating computer misuse than its originators intended.

## Introduction

It must be noted that obtaining information about the prosecutions brought under the *Computer Misuse Act* 1990 is a rather difficult matter, as most of the recent cases have not been reported in recognised law reports, having been resolved in the lower courts. This means that any research in this area has to lean heavily upon coverage drawn from national daily newspapers and trade papers. These outlets are often selective in the content and style of their coverage, having their own idiosyncratic reasons for publishing information and opinions. The view of the state of the law are expressed by such bodies is often confused and sometimes inaccurate. Shorthand transcripts of the individual cases are often available, but these may cost up to £400 per day of trial to have prepared. The case of *R v*

*Bedworth and others* lasted for about three weeks.

The issue of computer crime is fraught with difficulties. Not the least of these is the matter of establishing when the use of a computer in criminal activity goes beyond the use of any other device, electronic<sup>3</sup> or otherwise, to aid a person in the commission of an offence, and becomes something for which there are convincing grounds to label it a computer crime. Only at that point, it may be argued, is it justifiable to create a definition of computer crime which should have its own separate existence in the common law and in legislation.<sup>4</sup> This is a matter that has caused problems for both legislators and academic writers, and which has led to more than ten years of heated debate.<sup>5</sup> This debate has significantly affecting the way in which the current UK legislation on computer misuse has developed.

In the UK, the school of thought that stated that existing legislation<sup>6</sup> and the common law could deal adequately with the problems thrown up by the use of computers and information technology held sway until the later 1980's. Then, a small number of high profile cases began to highlight the difficulties in stretching existing categories of law to cover situation involving what may be best described as computer misuse, but which the general public and the media have come to call hacking.<sup>7</sup>

The background to the *Computer Misuse Act* 1990 Public attention was drawn to the issue of computer misuse by the media's extensive coverage of *R v Gold and Another*<sup>8</sup> where the

limitations of the then existing law to deal with computer hacking led to the eventual acquittal of the defendants. The defendants had hacked into a computer databank, using customer identification numbers and passwords that they had obtained without numbers and passwords that they had obtained without permission. Upon entering the system they obtained information without payment and altered data without authority. They were charged and initially convicted under the *Forgery and Counterfeiting Act* 1981 ss1, 8(1)(d) on the grounds that when the customer identification numbers and passwords were keyed in, the computer held them momentarily while checking them, then irretrievably deleted them upon the entrance of the defendants to the system. This, it was claimed by the prosecution, was

'making a false instrument, with the intent of using it to induce the databank to accept it as genuine to the prejudice of the company operating the system.'<sup>9</sup>

The House of Lords, however, upheld the Court of Appeal's decision in quashing the convictions, on the ground that,

'A device could not be an instrument under 8(1)(d) of the 1981 Act by which the information was recorded or stored by electronic means, unless it preserved the information for an appreciable time with the object of subsequent retrieval or recovery. Since the momentary holding of the customer identification numbers and passwords while they

were verified did not amount to the recording and storage of information, the respondents had not made an instrument within s8(1)(d) and could not be guilty of an offence under s1.<sup>10</sup>

The outcome of that case in particular, and the issues raised in previous cases such as *Cox v Riley*<sup>11</sup> and *R v Whitely*<sup>12</sup>, concerning the difficulties in using the *Criminal Damage Act* 1971 where there was damage to intangible rather than tangible property<sup>13</sup>, led to increasing pressure for legislation to bring the criminal law up to date with technology. This pressure resulted in a referral to the Law Commission which produced a report, Report No. 186, Computer Misuse<sup>14</sup>. This was followed by a Private Member's Bill sponsored by Michael Colvin MP. The Bill was put before Parliament to implement the Commission's recommendations and became the *Computer Misuse Act* 1990.

### **The Computer Misuse Act 1990**

The Act creates three new offences, and was designed to avoid the 'tangible evidence' difficulties. The sections creating the new offences are as follows:

1. (1) A person is guilty of an offence if:
  - (a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;
  - (b) the access he intends to secure is unauthorised; and
  - (c) he knows at the time when he causes the computer to perform the function that that is the case.
- (2) The intent a person has to have to commit an offence under this section need not be directed at:

- (a) any particular program or data;
- (b) a program or data of any particular kind; or
- (c) a program or data held in any particular computer.

- (3) A person guilty of an offence under this section shall be liable on summary conviction to imprisonment for a term not exceeding six months or to a fine not exceeding level 5 on the standard scale or to both.

Thus, Section 1(1) clearly makes hacking an offence, and Section 1(2) states that there need be no inten-

### ***"The Act creates three new offences, and was designed to avoid the 'tangible evidence' difficulties"***

tion to cause harm. However, this is only a summary offence and thus on conviction the maximum imprisonment possible is no more than 6 months and the maximum fine £5,000. The limited penalties available under this section have been partially responsible for the problems in utilising the Act. Sections 2 and 3 contain the more serious offences. Section 2 applies to unauthorised access with intent to commit, or aid the commission of an offence, and Section 3 concerns the unauthorised modification of the contents of any computer.

2. (1) A person is guilty of an offence under this section if he commits an offence under section 1 above ('the unauthorised access offence') with intent:

- (a) to commit an offence to which this section applies; or
- (b) to facilitate the commission of such an offence (whether by himself or by any other person);

and the offence he intends to commit or facilitate is referred to below in this section as the further offence.

- (2) This section applies to offences:

- (a) for which the sentence is fixed by law; or

- (b) for which a person of twenty-one years of age or over (not previously convicted) may be sentenced to imprisonment for a term of five years (or, in England and Wales, might be so sentenced but for the restrictions imposed by section 33 of the *Magistrates' Courts Act* 1980).

- (3) It is immaterial for the purposes of this section whether the further offence is to be committed on the same occasion as the unauthorised access offence or on any future occasion.

- (4) A person may be guilty of an offence under this section even though the facts are such that the commission of the further offence is impossible.

- (5) A person guilty of an offence under this section shall be liable:

- (a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both, and

- (b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

3. (1) A person is guilty of an offence if:

- (a) he does any act which causes an unauthorised modification of the contents of any computer; and
- (b) at the time when he does the act he has the requisite intent and the requisite knowledge.

(2) For the purposes of subsection (1)(b) above the requisite intent is an intent to cause a modification of the contents of any computer and by so doing:

- (a) to impair the operation of any computer;
- (b) to prevent or hinder access to any program or data held in any computer; or
- (c) to impair the operation of any such program or the reliability of any such data.

(3) The intent need not be directed at:

- (a) any particular computer;
- (b) any particular program or data or particular kind; or
- (c) any particular modification or a modification of any particular kind.

(4) For the purposes of subsection (1)(b) above the requisite knowledge is knowledge that any modification he intends to cause is unauthorised.

(5) It is immaterial for the purposes of this section whether an unauthorised modification or any intended effect of it of a kind mentioned in subsection (2) above is, or is intended to be, permanent or merely temporary.

(6) For the purposes of the *Criminal Damage Act 1971* a modification of the contents of a computer shall not be regarded as damaging any computer or computer storage medium unless its effect on that computer or computer storage medium impairs its physical condition.

(7) A person guilty of an offence under this section shall be liable:

- (a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statu-

*"Where the Act has been used, it appears to have been used with limited success"*

tory maximum or to both; and

- (b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

As can be seen, the penalties for offences under Sections 2 and 3 are considerably more severe. A conviction on indictment can lead to unlimited fines and up to five years imprisonment. It is important, however, to note that under Section 3(1)(b) the different degree of intent on the part of the defendant that the prosecution has to prove. It is possible that proving this degree of intent may now be becoming a potentially fatal problem for the *Act*.

It is important to remember that during its passage through Parliament, the original Private Member's

Bill, which was the basis for the *Computer Misuse Act 1990*, was considerably amended<sup>15</sup>. This rather piecemeal process of legislation has led to claims that the *Act* is no longer (or indeed never was) capable of achieving the purpose for which its originators intended it, namely the control of computer hacking<sup>16</sup>.

### ***The courts and computer misuse***

The records show, that, since its coming into force in August 1990, the *Act* has not been used to extent that the increasing reports of hacking in the media might suggest would be necessary.<sup>17</sup> Where the *Act* has been used, it appears to have been used with limited success.<sup>18</sup> Even when convictions are gained, sentences have been light when compared to the losses caused. In June 1992 a defendant who cost his victim, a typesetting firm, £36000 in lost business was given a conditional discharge and a £1 650 fine,<sup>19</sup> and in December 1992 a computer programmer who planted a logic bomb in his former employer's computer system causing £30 000 worth of damage was sentenced to 140 hours community service and ordered to pay £3 000 compensation.<sup>20</sup> Such sentences have been greeted with derision among computer professionals.<sup>21</sup>

The reasons why the *Act* has failed to make an impact are complex. While the media may occasionally sensationalise the problem, and over-emphasise its scale, there has clearly been an increase in computer misuse. This is due to a number of factors: the increasing computerisation, and more importantly, networking, of the workplace, with the attendant increase in the ability of computer literate employees to misuse that equipment to their employer's detriment; also to drop in

prices,<sup>22</sup> and rise in the computational power and connectability, of the home computer via national and international networks.<sup>23</sup> However, the increase in computer misuse often remains hidden as far as the law is concerned, for a number of reasons, not least of which is the difficulty in obtaining evidence. Firms are often unwilling to co-operate with the police for fear that they will suffer from adverse publicity if prosecutions result. Firms may make their own provision for dealing with computer misuse with internal penalties such as demoting or firing potentially embarrassing external investigation. Financial losses, on a small scale, may simply be written off as expected operating losses.

The response of the police to the computer crime has also been criticised. While Scotland Yard has a special computer crimes unit consisting of up to 80 officers,<sup>24</sup> both it and the efforts of the police have been criticised for lack of funding, manpower and expertise. The police response to this is that computer misuse cases are extremely time and resource consuming, and that those responsible for the *Computer Misuse Act* appeared to have little concept of how difficult it would be both to trace, and build a case against, suspected hackers.<sup>25</sup> An example given of this lack of foresight is the difficulty in carrying out surveillance, as the consent of both the victims and British Telecom is needed before an operation can go ahead.<sup>26</sup> It is also possible that sheer numbers of cases may be creating problems.<sup>27</sup>

In addition to this, the public and those involved in the legal system, particularly the judiciary, do not appear to be aware of the potentially highly destructive consequences of hacking. The consequences the public might think of, such as that envisaged in the movie 'Wargames',

with teenagers setting off World War Three by accident, are improbable, but businesses who have engaged in extensive computerisation, and who have limited or no 'disaster procedures' may simply not be able to function in the event that, for whatever reason, their computer system is unavailable. An American survey reported in *Computing* magazine in 1992 claimed that 85% of companies which experience a major breakdown in their computer systems fail to recover and go out of business within 18 months<sup>28</sup>. This may be due to loss of vital business information such as client lists and lists

---

***"...85% of  
companies which  
experience a major  
breakdown in their  
computer systems  
fail to recover and  
go out of business  
within 18 months"***

---

of outgoing deliveries, or the fact that the business is run more or less entirely electronically and thus cannot be delivered in any other form, or that repair costs are large enough to cripple the business. Often in the case of computer misuse perpetrated by outsiders, huge bills may be run up for use of services such as telephone lines.

#### ***R v Bedworth and the 'addiction defence'***

The recent acquittal of Paul Bedworth, a 19 year old artificial intelligence student studying at Edinburgh University, of three charges of conspiracy under the *Computer*

*Misuse Act* 1990 (and the 19th Century Telegraphy Acts), has raised considerable doubts about the effectiveness of that Act to curtail adequately the activities of computer hackers.

The history of the case is as follows:

On 26 June 1991 'Operation Killern' was mounted by police from four different forces. The three defendants, who were members of a hacking group called Eight Legged Groove Machine (8LGM), were arrested at their home addresses at around midnight. The prosecution alleged that all three were arrested in the act of committing an offence<sup>29</sup>. Computer equipment and documentation were seized at all the defendants' homes.

The three were charged with conspiracy to commit offences contrary to Section 3 of the *Computer Misuse Act* 1990 the prosecution alleging that Bedworth and his co-defendants had gained unauthorised access to the computer systems of academic, government and commercial organisations and modified the systems to which they gained access. They were also charged with conspiracy to make dishonest use of services provided by British Telecom. The prosecution accepted that none of the defendants hacked for gain or for any other criminal purpose. The defendants had never actually met, but they had communicated via electronic bulletin boards.

The sample offences they were charged with related to five institutions: Brighton Polytechnic, Bristol Polytechnic, The European Organisation for the Research and Treatment of Cancer (EORTC) in Belgium, the European Economic Community in Luxembourg, and the Financial Times. It was alleged during the trial that Bedworth had made changes to the code of a share index

database at the Financial Times which cost £25,000 to repair. He had also disrupted important research work by overloading the EORTC's computer and left the organisation with a £10,000 phone bill.

Bedworth's two co-defendants, Strickland and Wood, pleaded guilty to the conspiracy charge under s3 of the Act and to the charge of conspiring to obtain unlawfully telegraphic services. Bedworth pleaded not guilty. Bedworth's defence to the charges was to claim that he was addicted to computer use and by virtue of that addiction was unable to form the necessary intent. His counsel called as an expert witness, Professor Griffith Edwards of Maudsley Hospital, a leading expert in the field of addiction who had conducted a Psychological Assessment Interview with Bedworth to establish whether Bedworth suffered from some form of computer addiction or dependency. The concept of computer addiction has been discussed before, in terms of the fact that the obsessive use of computers might well constitute some form of addiction, and a book on this subject published in 1989 termed this suggested addiction 'computer tendency syndrome'<sup>30</sup>. However both book and theory have been criticised, and other scientific studies are still felt to be in their infancy<sup>31</sup>. Professor Edwards himself appears to have had some doubts as to how accurately it would be possible to judge, at present, the long term effects of 'computer addiction'.

The defence claimed that Bedworth's inability to engage in normal social relations leading to his isolation from his peer group resulted in him going 'to earth with his computer', and resulted in his becoming addicted to computer hacking. However, the issue of non-chemical dependence is one fraught with difficulties, not

the least of which is proving that any dependence exists in any one particular case. It seems that the medical evidence presented by the defence suggested that the following pointers (taken as a whole rather than as a simple checklist) should be considered: Does the subject have a subjective awareness of dependence? Are there behavioural manifestations? Is the length of time spent engaged in the activity unusual or abnormal? How does the subject behave when unable to carry out that activity? And is there any explanation, other than compulsion, for the relevant behaviour?

Computer misuse certainly appears to have overtones of other addictive

### *"Computer misuse certainly appears to have overtones of other addictive behaviour"*

behaviour. The backer ethos of individuals against the system certainly resembles other addict subcultures and the concept of repetitious behaviour leading to some kind of intermittent reward can clearly be seen to be habit forming. In the case of computer addiction, it could be argued, the particular action may be, for example, attempting repeatedly to crack a password, just as the avid gambler repeatedly attempts to win the jackpot on a 'one armed bandit'. The pleasure does not appear to come as a result of the consequences of a successful action ie. being able to access a computer system at will or winning the jackpot. Indeed the computer addict may have no great interest in a computer system's content, as a gambling addict may achieve no financial benefit from the

jackpot having placed more money in the machine than he has won. The primary pleasure seems to be in the perception of having somehow triumphed over the odds in the achieving of that successful action. In the case of the hacker, that is to have beaten the defences designed specifically to keep intruders out.

In Bedworth's case, he was said in his Psychological Assessment Interview to have made unprompted statements such as 'I believe I am addicted to hacking'<sup>32</sup>. Evidence was also submitted that he spent abnormally long hours in the computer laboratory at Edinburgh University (indeed, when permitted to do so by the University authorities, he would stay through the night), that his computer activities took precedence over all other activities, and that he had made statements to the effect that he felt uncomfortable and frustrated when not able to hack and that he had a need to hack even when he perceived that this might be antisocial or illegal behaviour. Those facts certainly fit the above criteria for addiction and appear to have convinced the jury that Bedworth was in fact addicted and thus unable to form the relevant intent. This, despite a summing up by Judge Michael Harris in which he made it clear to jurors that obsession and dependence could not be used as a defence to criminal charges.

It is certainly difficult to link such an addiction defence with any existing defence to a crime of specific intent, other than perhaps intoxication. Indeed, in cases of chemical dependency, the courts have been profoundly unsympathetic to the attempted use of addiction even as mitigation in sentencing on conviction of a criminal offence, let alone as a defence. In the case of *R v Lawrence*<sup>33</sup> the Court of Appeal was quite definite:

'We cannot make too plain the principle to be followed. It is no mitigation whatever that a crime is committed to feed an addiction, whether that addiction be drugs, drink, gambling, sex, fast cars or anything else. If anyone hitherto has been labouring under the misapprehension that it was mitigation, then the sooner and more firmly they are disabused of it the better.'

Richard Buxton QC, the Law Commissioner who drafted the original report which led to the *Computer Misuse Act 1990* is reported to have called the result 'a fluke', suggesting that as the judge appears to have directed the jury properly, the verdict was a result of 'the jurors having ideas of their own'<sup>34</sup>. It may be therefore a comparable case to that of *R v Ponting*<sup>35</sup> where a civil servant was prosecuted under s2 of the *Official Secrets Act 1911* for passing confidential documents regarding the sinking of the Argentine cruiser General Belgrano, during the Falklands conflict, to an opposition MP. In that case the jury, in apparent defiance of a summing up by the trial judge<sup>36</sup> that suggested that there was little option on their part but to convict the defendant, appear to have decided the case according to their own criteria. Partly as a result of this verdict, itself regarded at the time as an aberration, s2 of the *Official Secrets Act 1911*, which was increasingly regarded to be hard to obtain convictions under, was replaced by the *Official Secrets Act 1989*.

What the criteria used by the jury in *R v Bedworth* in fact were, is something we are unable to find out. If the acquittal was on the grounds that the jury believed that Bedworth was addicted to computer use to the extent that he could not form the necessary intent, it may be useful to examine the case in the light of writings on public attitudes towards

white collar crime with relation to computers<sup>37</sup>. We may, for instance, contrast this case with a hypothetical situation where a drug addict had broken into the Financial Times and in his search for things to steal, to raise money to feed his habit, damaged computer equipment causing £25,000 of damage, or had disrupted the important research work of the EORTC and left them with a bill for £10,000. Given the type of hostile summing up by the judiciary as evidenced above, it is difficult to see a jury acquitting that person on the grounds on which Bedworth appears to have been acquitted. That

*"Thus it may be argued, the image of the hacker has temporarily been elevated to the status of a kind of folk hero..."*

would give weight to the argument that the public still do not see computer misuse crimes as particularly serious, even where one of the victims is a charity, and that the picture the public has of hackers is that of individuals 'bucking the system' through some form of eccentric flawed genius. Such activity is clearly damaging to the organisations who become victims, but the public perception the prosecution has to overcome, is that because they are large organisations they can absorb the costs without harm. This leads to the further perception that to pursue the individual causing that harm, while it may be legally correct, is unduly onerous. Thus it may be argued, the image of the hacker has temporarily been elevated to the sta-

tus of a kind of folk hero, a new age Robin Hood or perhaps more correctly a Dick Turpin figure, an electronic outlaw<sup>38</sup>.

On the other hand, it could equally be argued that the real cause of the acquittal was simply jury sympathy for one effectively portrayed by his defence as a sad and lonely white middle-class boy whose only contact with the world was via computers (my words) who, through mischievous, but not malicious, behaviour, caused damage to others without really being aware of the consequences of his actions. This view would be bolstered by the evidence presented that Bedworth was now of the opinion that he had been wrong to hack, that he was suitably penitent when questioned about his misdemeanours and had made statements to the effect that he would not repeat his illegal actions. In that case, the addiction defence could be seen as no more than a convenient excuse to reach the decision to acquit.

Bedworth's acquittal has led to criticism of the Crown Prosecution Service's (CPS) decision to charge the defendants under s3 and not under s1, as it is claimed that if they had been charged with hacking under s1 of the *Act*, a guilty verdict would have been more likely as his actions fell clearly within its scope<sup>39</sup>, and it is suggested that the CPS would have had to prove a lesser degree of criminal intent. It seems that the CPS's decision to charge the defendants with conspiracy under s3 was taken due to the fact that the group had engaged in hacking on such a massive scale. This resulted in the prosecution having to prove that the defendants had both the 'requisite intent and the requisite knowledge' required by s3(1)(b), a task with potentially more pitfalls. Given the uncertainties of exactly why the jury chose to acquit Bedworth, it is per-

haps rather harsh to blame the CPS for this 'mistake', as the question of the exact degree of intent and knowledge required may not ultimately have been particularly relevant to their decision.


Whatever the jury's reasoning, there is understandably considerable concern about this verdict and the effect that it will have on the future application of the *Computer Misuse Act*. It has been described by some as a 'licence to hack'<sup>40</sup>, and the addiction defence has been viewed with some scepticism as yet another loophole in an *Act* already seriously, if not fundamentally, flawed. However, despite the reports that Bedworth's counsel, Alistair Kelman, is of the opinion that the addiction defence is a viable one, and that it might also be used to help other addicts including those with chemical dependencies, in cases which require the prosecution to prove specific intent<sup>41</sup>, it is difficult to see the courts being willing to accept such a radical change. In somewhat different circumstances, in the case of *R v Llandudno Justices for the Petty Sessional Division ex parte Prenton*<sup>42</sup> the Court noted obiter that if,

'intoxication was a defence to offences of non-specific intent then a coach and horses would be driven through the criminal law of this country. It would be a serious matter if confined only to the compulsive alcoholic drinker, but drug addiction is even more compulsive and if ... submissions were right a seriously affected drug addict would have a defence to any crime of non-specific intent and that would be a very serious situation indeed.'

It would therefore seem reasonable to conclude, given the highly negative response in that case to the suggestion that involuntary intoxication

by virtue of addiction could be a defence to offences of non-specific intent, that the courts will be minded to treat a not dissimilar computer addiction argument regarding crimes of either non-specific or specific intent (that is, that the defendant could not stop himself from engaging in computer hacking due to some form of computer addiction), as at least equally undesirable.

### Conclusion

While the Bedworth case has raised the controversy surrounding *Computer Misuse Act* 1990 to new levels<sup>43</sup>, it seems unlikely to have significant long term consequences with regard to the viability of the addiction defence and the question of intent. The future of the *Act* as a viable method of combating computer misuse is more likely to be determined by the ability of the CPS to prosecute those arrested in the recent Operation Apache raids, coordinated by Scotland Yard's computer crime unit, against suspected computer virus authors throughout the UK<sup>44</sup>. Indeed, success or failure in prosecuting those concerned will be of greater significance in assessing whether it is finally time for Parliament to reconsider the whole issue of legislating against computer misuse. 

*Andrew Charlesworth is a lecturer at the University of Hull Law School, United Kingdom.*

### Footnotes

<sup>1</sup> I should like to thank Holly Cullen, William Lucy, David Freestone and John Lambert of the University of Hull Law School for their suggestions and advice while I was writing this article. Any mistakes remain, of course, my own.

<sup>2</sup> Unreported.

<sup>3</sup> For example the use of a pocket calculator in fraudulent financial activity.

<sup>4</sup> Wasik M. *Crime and the Computer* Oxford 1991 p1-4.

<sup>5</sup> It is not proposed to examine this issue in depth in this paper, for a further elaboration, see Wasik M. *ibid.* p. 1-6 for a discussion of this ongoing debate.

<sup>6</sup> Notably the Criminal Damage Act 1971.

<sup>7</sup> The term "hacker" and thus the concept of 'hacking' has undergone a radical shift in meaning. As far as computing terminology is concerned, it was initially used to describe 'A person who enjoys exploring the details of programme systems, and how to stretch their capabilities, as opposed to most users who prefer only to learn the minimum necessary'. It is more usually understood now as a 'A malicious meddler who tries to discover sensitive information by poking around'. Both these definitions and six others are to be found in Eric Raymond (\*ed.) *The New Hackers Dictionary*, MIT Press, 1991. Martin Wasik in *Crime and the Computer op. cit.* at 18, attributes virtually identical definitions to J. J. Bloombecker in 'Crime Update' *The View as we Exit 1984* (1085) 7 *Western New England Law review* 627 at 629.

<sup>8</sup> [1988] 2 A.; ER 196 (HL).

<sup>9</sup> *ibid.* at 186.

<sup>10</sup> *ibid.*

<sup>11</sup> (1986) 83 Cr App Rep 54.

<sup>12</sup> *The Times* 25 May, 8 June 1990 see also *R v Whitley* (1991) 93 Cr App Rep 25 (CA).

<sup>13</sup> That is, damage to, or destruction of, software or data held on a computer or on storage media in electronic form rather than damage to the computer or storage media itself.

<sup>14</sup> Published in October 1989.

<sup>15</sup> For Parliamentary debate see *Hansard HC vol. 166, cols. 1134-84, vol. 171, cols. 1287-339 and HL. Vol. 519, cols. 230-47.*

<sup>16</sup> Most notably by Emma Nicholson MP, a stalwart campaigner for improved measures against computer misuse.

<sup>17</sup> Although these reports tend to be rather sporadic, influenced by events such as the Bedworth case, with on computer trade journals maintaining some sort of long term consistency in reporting. The first conviction under the *Act* was that of Ross Pearlstone who had hacked into Mercury systems. He was fined £900.

<sup>18</sup> Partly because of judicial uncertainty over the application of the *Act* to hacking. Sean Cropp, who was the first person charged under the *Act*, was acquitted when the judge decided that hacking could only take place when one computer accessed another. This decision was later overruled by the Court of Appeal in *Attorney General's Reference (No 1 of 1991) (CA)* [1992] 3 WLR 432.

<sup>19</sup> 'Bedworth case puts law on trial' *Computing* 25th March 1993 p7.

<sup>20</sup> 'Bomber walks free despite Guilty verdict' *Computing* 10th December 1992 p3



<sup>21</sup> Although it may be argued that losses caused in criminal cases are often not a large factor in sentencing, and that the computer media's attitude merely reflects a misunderstanding of the practice of sentencing.

<sup>22</sup> 'Bedworth allegedly hacked his way around the world using a £200 BBC Micro, a computer that went into thousands of homes and schools in the early Eighties. In 1984, two Los Angeles teenagers were arrested for hacking into the Pentagon's Advanced research Projects Agency Network - one of the most secure in existence at the time — using equipment costing about £150.' The Daily telegraph 1st March 1993.

<sup>23</sup> Hackers appear to be particularly fond of the UK Joint Academic Network (JANET) as a jumping off point to access both UK Higher Education institutions systems and other systems world wide.

<sup>24</sup> Although in the case of the 'artful dodger' Computer Weekly March 25th 1993 it is stated that the core of that special unit is being disbanded in the aftermath of the *R V Bedworth* case.

<sup>25</sup> Bedworth himself when questioned by police about his exchange of hacking data to his co-defendants via bulletin boards, is said to have retorted 'I'm free to exchange whatever messages I want on bulletin boards. It doesn't mean that I have actually committed a crime.' 'The case of the "artful dodger"' *ibid*.

<sup>26</sup> 'The case of the "artful dodger"' Computer Weekly *ibid*.

<sup>27</sup> In the article 'Cop calls for help in Virus battle' in Computing March 4th 1993 p 7 Detective Inspector John Austen, head of Scotland Yard's Computer Crime Unit is reported to have claimed that his unit lost count of the number of incidents of computer crime in the UK, but that the number was at least 30 000 and rising. It is necessary, however, to treat all such reported figures with a degree of caution as there is often no clear indication of what type of activities are being covered by the term 'computer crime' or indeed the degree of their severity.

<sup>28</sup> Computing 22 October 1992 p27. However, this study was referred to only briefly, and it is thus difficult to determine the extent to which the computer system breakdown was the prime or only factor in the failure of individual companies, or indeed the [ ] of instances which involved hacking.

<sup>29</sup> 'Hacker Gang jumped off Digital's Line' Computing 11th March 1993.

<sup>30</sup> M. Shotton, *Computer Addiction? A Study of Computer Dependency*, London: Taylor & Francis 1989.

<sup>31</sup> Clinical studies in chemical dependence, ie. drug and alcohol dependence, have been run for periods of over 20 years, allowing scientist to determined by observation some clear characteristics of dependency in those circumstances. Clinical studies in non-chemical dependence, especially relating to computer use, are considerably more limited and the results so far unclear and disputed.

<sup>32</sup> Also in statements to police he was alleged to have said 'I can't top myself from doing it because it goes on and on and on and I can't stop. It's a kind of addiction.' - reported in 'I'm addicted says hacker' Computing March 4th 1993 at p3.

<sup>33</sup> [1989] Crim. L.R. 309 (CA). This case involved an appeal against sentencing, on the grounds that the appellant committed burglaries solely to support his heroin addiction, and that this should have been taken into account by the Court of first instance as a mitigating factor. Leave to appeal had been given because the judge felt that 'there seems to be scant authority on the question of whether and to what extent, the fact that burglary was solely to feed drug addiction, could be a mitigating factor'. Other factors suggested as subsidiary grounds of appeal were that the appellant had made frank admissions to the police upon arrest and that he was had been drug free for 8 months at time of trial. Interestingly, these grounds, rejected outright by the Court of Appeal, would also seem to echo some of those put forward by Bedworth's counsel.

<sup>34</sup> 'The case of the "artful dodger"' Computer Weekly *op. cit*.

<sup>35</sup> [1985] Crim. L.R. 318.

<sup>36</sup> The view of those who might term themselves hackers themselves is for practical reasons virtually impossible to determine, and it appears as yet that the acquittal of Bedworth has done little to excite debate on the issue. 'Hackers stay quiet on court acquittal' The Times March 19 1993 p5. However, much of the 'outlaw' imagery appears to be a creation of both the media and of SF authors notably William Gibson (who tends to get a mention in many hacker related articles).

<sup>37</sup> See the studies referred to in Wasik M. *Crime and the Computer* *op. cit*. pp. 22-33.

<sup>38</sup> The view of those who might term themselves hackers themselves is for practical reasons virtually impossible to determine, and it appears as yet that the acquittal of Bedworth has done little to excite debate on the issue. 'Hackers stay quiet on court acquittal' The Times March 19 1993 p5. However, much of the 'outlaw' imagery appears to be a creation of both the media and of SF authors notably William Gibson (who tends to get a mention in many hacker related articles).

<sup>39</sup> 'The case of the "artful dodger"' Computer Weekly *op. cit*., 'A law lacking conviction' (Editorial) Computing 25th March 1993 p13.

<sup>40</sup> 'Bedworth case puts law on trial' Computing *op. cit*.

<sup>41</sup> 'The case of the "artful dodger"' Computer Weekly *op. cit*.

<sup>42</sup> 16 May 1986. Unreported (Transcript: Marten Walsh Cherer on LEXIS) QBD. The case concerned a request for an order of judicial review in respect of two convictions for criminal damage. The primary question before the Court is not in itself directly relevant to this article, being whether drunkenness by virtue of alcoholism amounted to voluntary intoxication or self induced intoxication for the purposes of the rule in *DPP v Majewski* [1976] All ER 142.

<sup>43</sup> For instance, a British Computer Society vice chairman is quoted as saying '... the BCS is convinced that the operation of the Act urgently needs to be reviewed. This review should be carried out from the point of view of the capabilities and practices of the investigating and prosecuting authorities, including the Police and the Crown Prosecution Service. It should also examine the terms of the actual wording of the Act itself. The BCS will of course collaborate with the appropriate authorities in a review, and urges the Home Office to create an adequately resourced and qualified task group for this purpose without delay.' in 'BCS voices views on hacker trial' BCS News in Computing 15th April 1993.

<sup>44</sup> 'Apache scalps virus cowboys' Computing 11th Feb. 1993 p1.