The Computer Misuse Act 1990: lessons from its past and predictions for its future

Macewan, NF

Criminal Law Review

2008

The Computer Misuse Act 1990: lessons from its past and predictions for its future

Neil MacEwan

Subject: Criminal law. **Other related subjects:** Information technology

Keywords: Computer crime; Computer security

Legislation: Computer Misuse Act 1990 s.1 , s.3
Police and Justice Act 2006 s.35 , s.36

***Crim. L.R. 955** **Summary:** *The age of the internet has thrown down some real challenges to the Computer Misuse Act 1990. Recently, the Government made changes to this piece of legislation, in an attempt to meet two of those challenges--the proliferation of " Denial of Service" (DoS) attacks, and the creation and dissemination of " Hackers' tools" --and to fulfil international commitments on cybercrime. Yet some of these new measures invite criticisms of policy, form and content, and bring doubts about how easy to interpret, and how enforceable, they will be.*

Introduction

Finally, after three aborted attempts to make changes to it within the last five years,[1] the Computer Misuse Act (CMA) 1990 has been amended; specifically, both added to and altered.[2] The offence of *unauthorised access to computer material,* [3] formerly a summary offence, has now become an offence triable either way, and the offence of *unauthorised modification of computer material* [4] has been replaced by the offence of *unauthorised acts with intent to impair, or recklessness as to impairing, the operation of a computer etc.* The time is right for a close re-examination of this piece of legislation.

The CMA came into force on August 29, 1990. Soon after, the Court of Appeal delivered its judgment in *Whiteley,* [5] in which it found no difficulty in confirming a hacker's conviction under s.1 of the Criminal Damage Act (CDA) ***Crim. L.R. 956** 1971. That judgment undermined some of the claims put to, and made by, the Law Commission regarding the perceived inflexibility of the CDA 1971 in such scenarios.[6] At the same time, it supported the arguments put in favour of simply amending the CDA 1971, or just leaving it be.[7]

Perhaps, at that point, the UK Government should have adopted a holding position, from which it could have taken more time and care in deciding how to legislate on hacking and other forms of computer misuse. The law could have been developed in a sensible fashion by the judiciary, while rigorous, credible studies of computer misuse could have been conducted. The resulting evidence would have given a clearer picture of the problem and, crucially, been open to widespread critical scrutiny. In addition, as time passed, the Government's steep learning curve would have enabled it to legislate in anticipation of the cyberspatial explosion which would soon come. Instead, the CMA suffered a premature birth, which left it weak and vulnerable when the internet, as we know it, arrived.[8]

The basis of the Act--system integrity

Hacking[9] can be viewed, inter alia, as invasion of privacy. However, in the United Kingdom, the criminal law has seldom been used in the protection of privacy.[10] In this respect, the CMA was anomalous in a system where no general right of privacy is recognised by the criminal law. When the CMA arrived, some had already questioned why the unauthorised access of confidential information held on a computer should be an offence where if the same information were held on card index no offence would be committed.[11]

Hacking has been seen as morally akin to breach of privacy, and legally akin to trespass.[12] Yet herein lies another anomaly. In English law, trespass is a *civil* wrong, a tort. It does not become a criminal offence without some further, aggravating feature. Yet the CMA did not

just criminalise hacking with intent to commit further offences. It also criminalised basic hacking--the computer equivalent of mere trespassory entry. In English law, neither words transmitted by electronic impulse, nor information--whether held within a computer or not--attain the status of property.[13] The debate about whether the law should directly address the ***Crim. L.R. 957** issue of " information theft" was ongoing when the CMA arrived[14] and continues to run.[15] However, in the late 1980s, both the English and Scottish Law Commissions left this area " well alone" .[16] The notion that criminal laws should be addressed to the concept of " information" and not confined to the integrity of the computer is a strong argument.[17] Moreover, the concept of a legal regime for information which is not derived from analogy with rules for corporeal objects has much to recommend it.

The conceptual basis of the CMA was, in fact, the protection of the integrity and security of computer systems. The Law Commission had concluded that " the case for a criminal offence of basic hacking [did] not turn on the need to protect information" .[18] It also took the view that " clarification of the law" was required concerning the destruction or alteration of information held within computers.[19] Was this a lost opportunity for some creative legislative thinking? The Law Commission seemed loath to delve into the complexities of " information law" theory. The calls for patience and greater inquiry, in the search for a better strategy, seemed to fall on deaf ears.[20] The truth is that the CMA offered the simplest route for law reform. It was a compromise between radical thought and minimal action.

The miscreant insider

The concept of " authority" remains the keystone of the Act. The access or modification (now " impairment" [21]) of programmes or data must be " unauthorised" .[22] If the accused was not entitled to control the process in question (access or modification/impairment), and did not have the consent of someone who was, the requisite lack of authority is established.[23]

Back in 1989, as it ushered in the Act, the Law Commission declared that the basic hacking offence (in s.1) was mainly aimed at the " remote" hacker, but was also " apt to cover the employee or insider as well" .[24] However, it is submitted that the application of the Act to " insiders" has, at times, been confused and inconsistent. *DPP v Bignell* [25] provides a focus for such criticism. The facts were simple. Mr and Mrs Bignell were both police officers. On six occasions, they instructed computer operators to extract information from the Police National Computer (PNC) for ***Crim. L.R. 958** them. They sought this information for private, unofficial purposes. The Police Commissioner had previously ruled that the PNC was to be used for police purposes only, and the Bignells knew this.[26] When their convictions were quashed, the DPP appealed by way of case stated to the Divisional Court, but without success. The court distinguished the activity of " breaking into computers" from the " misuse of data" . It took the view that the Bignells had indulged in the latter.

That decision invites strong criticism. The key issue was the true nature and extent of the authority which had been given to the defendants. The Divisional Court seemed adamant that the Bignells had authority to access the data in question, but that is debatable. Authorisation involves the giving of permission. That permission relates not only to the area of conduct but to the conduct itself within it. In his commentary on the *Bignell* case, J.C. Smith argued this same point by analogy: " If I give you permission to enter my study for the purposes of reading my books, your entering to drink my sherry would surely be unauthorised ' access' to the room as well as to the sherry" .[27]

Two years later, in *R. v Bow Street Magistrates' Court Ex p. Allison,* [28] the House of Lords was presented with an opportunity to review the *Bignell* decision. Their Lordships dealt with some of the remaining issues, but ducked others. They rightly criticised the Divisional Court for posing a wrong question; its focus should have been on whether the Bignells had authority to access the *actual* data involved, not merely the *kind* of data in question. Despite this, their Lordships went on to conclude that the decision in *Bignell* was " probably right" . Yet their stated reasons for this opinion were not wholly convincing. Lord Hobhouse declared that a " possible view of the facts" was that the access in this case was necessarily authorised because it was secured by the computer operators, who were authorised to

access the PNC in response to requests from police officers. But such focus upon the computer operators was implicitly misplaced. They were blissfully unaware of the real reason behind the Bignells' requests. In short, they were innocent agents. Some have stated that the doctrine of innocent agency was not applicable in this case,[29] while others think that it certainly was.[30] The latter opinion is the correct one. The fact that the computer operators lacked mens rea means that they should not have been viewed as participants in the alleged offences. In such circumstances, " the Principal is the participant in the crime whose act is the most immediate cause of the innocent agent's act" .[31] The Bignells fitted this description.

Certainly, the Law Lords' judgment in *Ex p. Allison* supported convictions in cases where police officers had *themselves* accessed the PNC for unauthorised purposes, such as in *Bonnett.* [32] However, at the same time it denied support to convictions in cases where, like the Bignells, defendants had asked others to access the data in question for them, such as in *Farquarson.* [33] Given the doctrine of innocent agency, there is no sustainable distinction between such cases. It has been ***Crim. L.R. 959*** disappointing to see confusion and lack of clarity in the application of the crucial concept of " authority" . This has somewhat undermined the Act.

Claims about loopholes in the Act

The very first prosecution under the CMA[34] raised concerns that it might have been built on sand. The decision had seismic implications for the foundations of the Act. However, at the request of the Attorney-General,[35] the Court of Appeal came to the Act's rescue by clarifying that it did not simply apply to " remote" hacking. In short, both direct *and* indirect unauthorised access would be caught in the legislative net. The decision in *Bedworth* [36] was dubbed by some a " Hacker's Charter," [37] the same label which had been attached to the influential, pre-Act case of *Gold and Schifreen.* [38] The truth is that this decision did not reveal a loophole in the Act. Rather, " a loophole occurred in the application of the ... Act" .[39]

A more legitimate claim of a lacuna concerned the issue of Denial of Service (DoS) attacks. These are launched against computer systems or networks to cause a loss of service to users, typically the loss of network connectivity by consuming the bandwidth of the victim network or by overloading its computational resources. They are not a new phenomenon.[40] A Distributed Denial of Service (DDoS) attack poses a more potent threat. This is where large numbers of remote computers, which have been infected,[41] are orchestrated to attack a target at the same time. These " Botnet army" manoeuvres have become very prevalent in recent times.[42] They can be used to extort money from organisations,[43] to further political protest,[44] or even as a means of inter-governmental cyber-warfare.[45]

There was considerable debate over whether the CMA covered such activities. However, it was said that the wide disparity in legal opinion was due to the fact ***Crim. L.R. 960*** that only the particular circumstances of each attack made it obvious whether the CMA wording applied.[46] The decision at first instance in the case of *Lennon* [47] provided judicial confirmation of a gap in the law. There, it was successfully argued that an email bombardment,[48] conducted by the disgruntled accused against the company from which he had recently been dismissed,[49] could not be caught by s.3 of the CMA, on the basis that the recipient machine was designed to receive and respond to such email messages and, therefore, his sending of (all of) them was " authorised" . That judgment was offered up as proof of the real need for reform of the CMA in this respect.[50] This perceived weakness of the Act drew much criticism from the media.[51] Such pressure contributed to the Government's recent decision to legislate further on the issue of DoS attacks. However, it is interesting to note that before these legislative changes were made, the decision in *Lennon* was successfully appealed by way of case stated. The Divisional Court remitted the case back to the District Judge on the basis that he had wrongly decided that there was no case to answer.[52] However, ultimately, the defendant entered a guilty plea, and legal clarity remained elusive.

Procedural difficulties

Computer crime is substantially under-reported.[53] There are a number of reasons for this.

First, corporate victims often wish to avoid the adverse publicity that could accompany a trial, much of which, in a sub judice situation, they could not fully rebut.[54] For example, an online banking service would be loath to advertise an apparent security weakness, fearing substantial loss of custom overnight. Such a revelation might also attract further attacks. Consequently, there is a clear risk of further loss and no prospect of any direct, economic benefit in a prosecution under ***Crim. L.R. 961** the CMA. Unlike a civil claim, it has no restitutional or compensatory element.[55] Indeed, reporting a crime may lead to " the consumption of much management time which could otherwise have helped make good the losses sustained" .[56]

If a victim company simply craves " justice" and deterrence, it may still be dissuaded by the distinct possibility that the perpetrator will not be convicted.[57] If the true culprit can be identified, the computer evidence could be subject to challenge in terms of its reliability, or could have self-destructed, damaging the system and leaving no admissible trace behind.[58] Difficulties might also arise where the offender sits in a country which does not have strong investigative, jurisdictional or extraditional links with the United Kingdom. According to the Confederation of British Industry, reasons such as these have, in the past, explained industry's ambivalence towards prosecuting those cases of computer crime which do come to light.[59]

Much regret was expressed about the Law Commission's scant consideration of the evidential and procedural problems associated with the use of computers.[60] Some computer-generated evidence can be difficult to obtain and/or difficult to adduce in court.[61] By its very nature, electronic data is vulnerable to destruction, deletion or modification. However, some legislative measures have been brought in to assist the task of gathering evidence.[62]

The response of the police to computer crime has attracted regular criticism.[63] Lack of funding, manpower and expertise remain weaknesses, notwithstanding the establishment of the National High Tech Crime Unit in April 2001.[64] Many of the respondents to the All Party Internet Group (APIG) inquiry in 2004 complained that the police were not giving sufficient priority to the investigation and prosecution of cybercrime. Indeed, it was pointed out that cybercrime was not one of the target measures by which police performance was assessed.[65]

Rates of prosecution

Despite the rise in computer misuse, there has been only a small number of prosecutions under the CMA. This is evidenced in the statistical information which ***Crim. L.R. 962** the Home Office supplied to the APIG inquiry in 2004. During the period from 1990 to 2006, in England and Wales, 214 defendants were proceeded against at magistrates' courts under the CMA,[66] and 161 were found guilty.[67] Although there has been some criticism of seemingly low conviction rates in prosecutions concerned with the CMA,[68] these figures show that the conviction rate in prosecutions where the *principal* offence with which the defendant was charged was a CMA offence (the aforementioned 214 prosecutions) is high (75 per cent). Yet criticism focusing on the *overall* lack of enforcement of the CMA is certainly not misplaced. Although the Law Commission stated that the justification for criminalising hacking lay in changing the climate of opinion, not necessarily in securing the conviction of a large number of individuals,[69] it applied this reasoning to the basic hacking offence alone.[70] Regarding the two, more serious offences, the law can only be a deterrent if it can be enforced effectively.[71] Given this, the low rate of prosecution under the Act warrants criticism.

Where convictions have been secured, the sentencing process has often come under fire.[72] Approximately two-thirds of s.1 convictions result in a non-custodial sentence.[73] Certainly, great damage can be done through computer misuse. This is particularly true of virus and worm attacks on the internet.[74] However, some commentators have doubted whether higher sentencing tariffs would significantly increase deterrence.[75]

The role of computer and network security

English criminal law is almost exclusively concerned with the conduct and culpability of the

offender.[76] However, criminologists have long since recognised the role of the victim in the " precipitation of crime" ,[77] and criminals' reliance upon the ignorance or carelessness of their victims.[78] It has been said that " the optimal protection … in cyberspace is a mix between public law and private fences" .[79] It is important to recognise computer and network security as a process, not a product. Technological measures such as properly configured firewalls, access control and ***Crim. L.R. 963** secure authentication should be supported by rigorous procedures, together with the encryption of critical data in storage and transmission.[80] In addition, detailed event logs and audit trails will help to provide cogent and admissible evidence for CMA prosecutions.[81] In short, security plays a crucial, pervasive role in the fight against computer misuse.

International initiatives on cybercrime

Certainly, since the arrival of the internet several years after the CMA's enactment, the Act has been looked upon as a piece of *cybercrime* legislation. Proper definition begins with the recognition that cybercrimes are not simply related to computers; they are *mediated* by *networked* computers. Consequently, it has been argued that the term " cybercrime" becomes far more meaningful when understood in terms of the *transformations* of acts by networked technology, rather than the acts themselves.[82] It used to be the case that criminal law was mainly driven and shaped by national interests alone. The global, decentralised internet, and the transjurisdictional criminality which it facilitates, have forced changes to this historical position. There has been a broad recognition of the need for a co-ordinated fight against cybercrime, and three organisations have formed a vanguard in pursuit of a harmonised approach: the Group of Eight (G8),[83] the Council of Europe,[84] and the EU Council.[85] It is within the context of these continuing international efforts that the recent changes to the CMA must be judged.

Are the changes to the CMA welcome?

Sections 35 and 36 of the Police and Justice Act (PJA) 2006 have changed ss.1 and 3 of the CMA. Section 35 transforms the summary offence in s.1 of the CMA into an offence triable either way. There are a number of reasons why this is a progressive move. It renders the offence extraditable, may increase deterrence through the raising of the sentencing tariff[86] and, in so doing, meets the requirement laid down in the EU's Framework Decision on attacks against information systems.[87]

***Crim. L.R. 964** The Government accepted APIG's recommendation that further legislation be brought in to criminalise DoS attacks, conscious also of its commitments under both the Cybercrime Convention[88] and the Framework Decision.[89] Section 36 of the PJA 2006 has done this by replacing the original s.3 of the CMA offence of " unauthorised modification" with one of " unauthorised impairment" .[90] Now, neither erasure nor modification of data are required to attract criminal liability. This steers the section further away from the troublesome concept of criminal damage, taking a more pragmatic view of data processing in the 21st century. The new, improved s.3 offence " shifts the locus of the crime from the ' contents of the computer' to potentially any point in a network which is held to be ' in relation to' the target computer" .[91] However, it is worth noting that the Cybercrime Convention refers to the " serious hindering" of computer systems,[92] and the Framework Decision to the " serious hindering or interruption" of information systems.[93] Yet the adjective " serious" does not feature within the new s.3 of the CMA. This casts a wider legislative net.

A more radical change can be found within this new s.3. Initially, in the early part of its journey through Parliament, the section was set to criminalise only *intentional* impairment of computer systems. However, a startling amendment to it was made in July 2006 during the Committee Stage of the Bill, whereby an additional, alternative form of mens rea was added. The new offence can now be committed with a reckless state of mind,[94] casting the net even wider. This extension of the criminal law to " reckless impairment" of computer systems could potentially muddy the interpretative waters and lead to some questionable attempts at prosecution. It seems anomalous to lessen the mens rea requirements for the new s.3 while neither the new s.1 nor the new offence in s.3A[95] make mention of " recklessness" . Moreover, both the Convention and the Framework Decision only call for an *intentional* state of mind to accompany such actions, as did the APIG inquiry.[96] Yet this

radical change was made at a late stage, protected from the rigours of wider public scrutiny. This could prove to be a costly example of legislative overkill. With this criticism in mind, it is also worth noting that the maximum term of imprisonment after conviction on indictment for this new offence is 10 years, which is 5 years more than that of the old s.3 offence. Indeed, APIG had recommended both a basic and an aggravated form of the new offence, the former carrying a maximum term of just 6 months' imprisonment and the latter carrying only 5 years' imprisonment.[97]

It is possible that the subjective concept of " impairment" could cause problems. It has been claimed that " the threshold at which decline in system performance ***Crim. L.R. 965** crosses the boundary into ' impairment' is likely to trouble the courts when considering the new section" .[98] Equally, once a system is rectified, proving that the requisite amount of " impairment" has occurred, and establishing causal linkage to the accused, could present real evidential difficulties.

Section 37 of the PJA 2006 has placed into the CMA a new offence of " making, supplying or obtaining articles for use in computer misuse offences" .[99] This meets the requirements of the Cybercrime Convention.[100] It targets the creation, supply and use of so-called " hackers' tools" .[101] It is this measure which has caused the most controversy beyond the walls of the Palace of Westminster. Notably, APIG advised the Government not to legislate on this particular matter.[102] The main problem stems from the fact that " researchers in information security, penetration testers[103] and other professionals in the field … may develop and make available such tools in the course of their study or business" .[104] In short, these items are easily accessible and are widely used for legitimate purposes on a regular basis. It seems that the courts will be left with the difficult task of drawing the line of their illegal use.

The mens rea requirements for the supplying offence within the section look flawed. People can attract liability where they supply, or offer to supply, such articles either intending them to be used to commit, or to assist in the commission of, an offence under either s.1 or 3, or believing it likely they will be so used. In short, mere belief is sufficient. This could be problematic. For example, when will a supplier's general knowledge that password recovery tools can be used for criminal ends cross the requisite threshold of belief in a specific case? This may seldom be an easy question for either magistrates or jurors to answer. However, the Government was determined to have these less stringent mens rea requirements for this offence. They were added to the section via an amendment tabled by a (then) senior Home Office Minister, Hazel Blears MP. When addressing concerns expressed about the correct interpretation of the word " likely" within the newly changed section,[105] she merely stated that " the word ' likely' is pretty well known in our legal system" .[106] This was a woefully insufficient response, revealing either little knowledge of, or perhaps wilful blindness towards, the difficulties which the courts have faced in defining terms of mens rea and those related to them. Ironically, when the debate moved to the House of Lords, the governmental view of what the word " likely" should mean in this context varied. Initially, the Home Office had stated that it meant " more likely than not" .[107] Later, however, Lord Bassam of Brighton advised that " [the word] ' likely' reflects a belief that there is a strong possibility" .[108] This lack of clarity fuelled criticism of the latterly inserted clause. The Earl of Northesk, a ***Crim. L.R. 966** parliamentarian with real knowledge of computer and cyberspatial issues, called for its removal on the grounds that it was " unnecessarily and dangerously broad" ,[109] but to no avail. One thing was clear: the Government wanted suppliers to think carefully--at least once, if not twice--about the people to whom they might sell.

Conclusion

The 18 year history of the CMA has revealed its flaws. Problems have emerged with its provisions and their practical application within the courts. Some of these cracks can be traced back to the process of inquiry which ushered in the Act. The Law Commission's task was not an easy one. Its investigation into this challenging subject was hampered by a dearth of reliable information. This led the Commission to seek confidential counsel from a number of interested parties after the inquiry's consultation period had officially ended. These dialogues profoundly influenced the Commission, prompting some remarkable changes of its collective mind. Yet the evidence and advice given to the Commission during

these secret soundings, and the Commission's response to it, was not available for wider, public scrutiny. Add to this the pressure for action which the Law Commission seemed to be feeling from several sources, and the fissures run deep.

The Act was born four years before the cyberspatial explosion that was delivered by the internet. This revolutionised many things, including computer misuse. Certainly, if the Law Commission's inquiry had been deferred to allow the collection of reliable statistical information on computer misuse, the lapse of time would have also delivered better foresight of the cybercriminal future. The CMA's main focus was on traditional hacking, an activity which has become something of a side show in the new millennium. Certainly, hackers can still pose a serious cybercriminal threat,[110] but broadband technology has prompted change within the cybercrime agenda.[111] Cybercriminals' engagement with victims is now more automated and asymmetric. New and more potent cybercrimes continue to emerge, their potency derived either from refinement or blending. For example, DoS attacks have been refined into DDoS attacks, launched by " Botnet armies" of computers which have been forcibly conscripted after falling victim to " blended threats" .[112] Some of the recent amendments to the CMA are attempting to respond to such developments.

It is important to remember that law is but one of the " four modalities of constraint" [113] which can be used to regulate cyberspace.[114] The digital realists claim that " more than law alone enables legal values, and law alone cannot guarantee them" .[115] The governments of many nation states have used those ***Crim. L.R. 967** modalities of constraint to effect significant control over cyberspatial activities within their territories. The predictions that the internet would be an unregulatable " forum without gatekeepers" [116] were wrong. The talk is now of the " bordered Internet" .[117] Yet this does not imply that global rules no longer have their place. On the contrary, it has been reiterated recently that " the cybercrime problem seems to require a global solution--international laws that prohibit computer invasions and disruptions, and that establish standards for international cooperation to redress the problem" .[118] In short, co-operation and harmony bring strength; international initiatives must continue to play a leading role.

The law, both national and international, legitimises the use of a range of techniques in the fight against cybercrime by " casting its shadow" over those other combative efforts.[119] Yet law which is outdated or simply difficult to enforce can fall into disrepute. The relatively small number of prosecutions under the CMA 1990 bears testament to this. For now, the Government has chosen to make amendments to this piece of legislation, both to address some of its perceived weaknesses and to meet international commitments on cybercrime. However, it is unlikely that the debate on " information law" will be defused by deferral. In the interim, the changes which the PJA 2006 has brought to the CMA 1990 will somewhat improve the chances of catching and convicting cybercriminals, and for this reason should be welcomed. However, the new provisions will also bring some problems of their own. A combination of some short-sighted, or simply stubborn, policy-making and some forceful government amendment during the Bill's passage through Parliament has produced certain provisions[120] which invite controversy, could sometimes prove difficult to interpret or enforce, and may lead to claims of legislative overkill.

Crim. L.R. 2008, 12, 955-967

---

1. May 1, 2002, April 5, 2005 and July 12, 2005.
2. Via ss.35-38 of the Police and Justice Act 2006. Although the PJA 2006 received Royal Assent on November 8, 2006, ss.35-38 did not come into force until October 1, 2008 (via The Police and Justice Act 2006 (commencement No.9) Order 2008). Note also that the Serious Crime Act (SCA) 2007 has amended PJA 2006 ss.35 and 36 by removing from them the offences of *enabling unauthorised access to computer material,* and *enabling acts with intent to impair the operation of a computer etc.* --see SCA 2007s.61(1), (2) and (3), respectively. Also, having abolished the common law offence of incitement (see s.59), the SCA 2007 has removed all references to offences of incitement from the CMA 1990--see SCA 2007 ss.6(3), 7(4), 8(3) and 9(2)(d).
3. The basic hacking offence in s.1.
4. In s.3.
5. *Whiteley* (1991) 93 Cr. App. R. 25.
6. See Confederation of British Industry, " Submission to the Law Commission on Working Paper No. 110 on Computer Misuse--The CBI Submission Part II" (1990) 6(2) *Computer Law and Security Report* 23, 24. See also Law Commission Working Paper No.110, *Computer Misuse* (1988), para.3.62.
7. See R. Brown, " Computer-related Crime Under Commonwealth Law, and the Draft Federal Criminal Code" (1986) 10 *Criminal Law Journal* 377; C. Tapper, " ' Computer Crime' : Scotch Mist?" [1987] Crim. L.R. 4; Law Commission Working Paper No.110, *Computer Misuse* (1988), para.1.4; H. Cornwall, " Hacking away at computer law reform" (1988) 138 N.L.J. 702; D. Bainbridge, " ComputerMisuse: What should the law do?" (1989) 133 S.J. 466.
8. In 1994/95.
9. This term has several meanings, but in this context is used to connote activities done in pursuit of unauthorised access to

computer programs or data.
10. R. Wacks, *Personal Information, Privacy and the Law* (1988).
11. M. Wasik, " Law Reform Proposals on Computer Misuse" [1989] Crim. L.R. 257, 260.
12. Tapper, " ' Computer Crime' : Scotch Mist?" [1987] Crim. L.R. 4, 19.
13. *Malone v Commissioner of Police of the Metropolis* [1979] Ch. 344 and *Oxford v Moss* (1978) 68 Cr. App. R. 183, respectively.
14. O. Bowcott, " New hacking law ' too hard to enforce" ' , *Guardian,* August 29, 1990, p.2; Wasik, " Law Reform Proposals on Computer Misuse" [1989] Crim. L.R. 257, 260.
15. A. Christie, " Should the Law of Theft extend to Information?" (2005) 69(4) J. Crim. L. 349; E. Wilding, " Hacked Off" (2006) 156 N.L.J. 753.
16. Cornwall, " Hacking away at computer law reform" (1988) 138 N.L.J. 702, 703.
17. Bowcott, " New hacking law ' too hard to enforce" ' , *Guardian,* August 29, 1990, p.2; B. Napier, " An end to hacking?" (1989) 133 S.J. 1554.
18. Law Com. No.186, *Computer Misuse.* Cm.819 (1989), para.2.13.
19. Law Com. No.186, *Computer Misuse.* Cm.819 (1989), para.2.28.
20. D. Bainbridge, " Hacking--The Unauthorised Access of Computer Systems: The Legal Implications" (1989) 52 M.L.R. 236; Bowcott, " New hacking law ' too hard to enforce" ' , *Guardian,* August 29, 1990, p.2.
21. The original CMA s.3 offence of " unauthorised modification" has now made way for the new s.3 offence of " unauthorised impairment" , inserted via PJA 2006 s.36.
22. CMA ss.1(1)(b), 2(1) and 3(1)(a).
23. CMA ss.17(5)(a) and (b), and 17(8)(a) and (b).
24. Law Com. No.186, *Computer Misuse.* Cm.819 (1989), para.3.35.
25. *DPP v Bignell* [1998] 1 Cr. App. R. 1.
26. At the very least, because it was stipulated in a manual which had been issued to them.
27. [1998] Crim. L.R. 54.
28. *R. v Bow Street Magistrates' Court Ex p. Allison* [2000] 2 A.C. 216.
29. M. Wasik, " Hacking, Viruses and Fraud" in Y. Akdeniz, C. Walker and D. Wall (eds), *The Internet, Law and Society* (2000), p.277.
30. I. Walden, *Computer Crimes and Digital Investigations* (2007), p.166.
31. D. Ormerod (ed.), *Smith and Hogan: Criminal Law,* 11th edn (2005), p.167.
32. *Bonnett,* unreported, November 3, 1995, Newcastle under Lyme Magistrates' Court.
33. *Farquarson,* unreported, December 9, 1993, Croydon Magistrates' Court.
34. *Cropp,* unreported, case note at (1991) 7 C.L.S.R. 168.
35. *Attorney-General's Reference (No.1 of 1991)* [1993] Q.B. 94.
36. *Bedworth,* unreported, May 21, 1993, Southwark Crown Court.
37. C. Christian, " Down and Out in Cyberspace" (1993) 90 L.S. Gaz. 2.
38. *Gold, Schifreen* [1987] Q.B. 1116.
39. Y. Akdeniz, *Encyclopedia of E-Commerce Law* (2005), para.15.007.
40. See, e.g. " Canadian Teen Charged in Web site attack released" , *CNN.com,* April 19, 2000, *http://edition.cnn.com/2000/TECH/computing/04/19/dos.investigation/index.html* [Accessed September 21, 2008].
41. By malware which has been delivered either by spam email or via " drive-by downloads" .
42. See the biannual Symantec Threat Report 2006, cited in " Denial-of-service hacking soars" , *BBC News,* March 9, 2006, *http://news.bbc.co.uk/go/pr/fr/-/1/hi/technology/4787474.stm* [Accessed September 21, 2008].
43. e.g. threatened attacks against online betting websites in the lead-up to the Grand National race (*http://www.timesonline.co.uk/tol/news/article1027674.ece* [Accessed October 13, 2008]) and the Cheltenham Festival (*http://www.theregister.co.uk/2004/03/17/online extortionists target cheltenham* [Accessed September 21, 2008]) in February and March 2004, respectively.
44. See, e.g. Hacktivists' attempt to disrupt ECHELON (the international electronic communications surveillance network) on Jam Echelon Day (October 21, 1999)--see C. Oakes, " Monitor This, Echelon" , at *http://www.wired.com/politics/law/news/1999/10/32039* [Accessed September 21, 2008].
45. See, e.g. the recent allegations of the Estonian Government that Russian authorities were responsible for a wave of attacks upon their websites, designed to make the Baltic State's systems crash and paralyse its infrastructure--see *http://www.timesonline.co.uk/tol/news/world/article1803847.ece* [Accessed September 21, 2008].
46. All Party Internet Group Report, *Revision of the Computer Misuse Act* (June 2004), p.10 (*http://www.apcomms.org.uk*).
47. *Lennon,* unreported, November 2, 2005, Wimbledon Magistrates' Court.
48. An example of a DoS attack.
49. Using a mail-bombing program named Avalanche, which he had downloaded from the internet.
50. T. Espinger, " Teenager cleared of email attack charge" , *ZDNet News,* November 2, 2005 (*http://news.zdnet.co.uk/security/0,1000000189,39235359,00.htm* [Accessed October 13, 2008]).
51. T. Espinger, " Denial of Service attacks are a legal ' grey area" ' , *ZDNetNews,* November 2, 2005 (*http://news.zdnet.co.uk/security/0,1000000189,39235148,00.htm* [Accessed October 13, 2008]); See also M. Whipp, " Computer Misuse Act crumbles as DoS attacker walks free" , *PC PRO News,* November 3, 2005 (*http://www.pcpro.co.uk/news/79505/computer-misuse-actcrumbles-as-dos-attacker-walks-free.html* [Accessed September 21, 2008]).
52. *DPP v Lennon* [2006] EWHC 1201.
53. See M. Levi, *Regulating Fraud* (1987), p.136; APIG Report, *Revision of the Computer Misuse Act* (2004), p.10; National Hi-Tech Crime Unit 2005 Survey at *http://www.nhtcu.org;* CSI/FBI 2004 Survey at *http://i.cmpnet.com/gocsi/dbarea/pdfs/fbi/FBI2004.pdf* [Accessed October 13, 2008]. See also D.S. Wall, " Mapping out cybercrimes in a cyberspatial surveillant assemblage" in F. Webster and K. Ball (eds), *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age* (2003), pp.112-136.
54. See Cornwall, " Hacking away at computer law reform" (1988) 138 N.L.J. 702; M. May, " How Hacking Law Could Weaken Security" , *The Times,* April 20, 1989, p.32; Department of Trade and Industry Report, *Dealing with Computer Misuse* (2002).
55. Y. Akdeniz, " Section 3 of the Computer Misuse Act 1990: An Antidote for Computer Viruses!" (1996) 3Web J.C.L.I. 7, *http://webjcli.ncl.ac.uk/1996/issue3/akdeniz3.html* [Accessed September 21, 2008].
56. Cornwall, " Hacking away at computer law reform" (1988) 138 N.L.J. 702.
57. Cornwall, " Hacking away at computer law reform" (1988) 138 N.L.J. 702.
58. Akdeniz, " Section 3 of the Computer Misuse Act 1990" (1996) 3 Web J.C.L.I. 6.
59. M. Wasik, " Conference Review: CBI Conference on Combating Computer Crime--Increasing Computer Security" (1989) 4(5) C.L.S.R. 4.
60. See B. Napier, " An end to hacking?" (1989) 133 S.J. 1554, 1556; I. Lloyd et al., " Computer Misuse: The Law Commission Report--Report on a seminar at Westminster with Emma Nicholson MP on 23 October 1989" (1990) 5(5) C.L.S.R. 9, 10.
61. See M. May, " Call to arms against the computer virus" , *The Times,* October 12, 1989, p.34; M. Wasik, " Law Reform Proposals on Computer Misuse" [1989] Crim. L.R. 257; E. Wilding, " Hacked Off" (2006) 156 N.L.J. 753.
62. e.g. s.12 of the Regulation of Investigatory Powers Act 2000, and the Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002 (SI 2002/1931).
63. See, e.g. Cornwall, " Hacking away at computer law reform" (1988) 138 N.L.J. 702; A. Charlesworth, " Addiction and hacking" (1993) 143 N.L.J. 540; APIG Report, *Revision of the Computer Misuse Act* (June 2004), p.10.
64. Now subsumed within the Serious Organised Crime Agency (SOCA).

65. APIG Report, *Revision of the Computer Misuse Act* (June 2004), p.15.
66. Note that these data are on the principal offence basis--see *http://www.apcomms.org.uk/apig/archive/activities-2004/computer-misuse-inquiry/computer-misuse-inquiry-written-evidence /Home Office - CMA regional stats.xls* [Accessed September 21, 2008]; see also *http://www. mams.salford.ac.uk/mams/p/?s=17&pid=69* [Accessed September 21, 2008].
67. In all courts.
68. See D. Rowland and E. Macdonald, *Information Technology Law,* 5th edn (2005), p.447; See also APIG Report, *Revision of the Computer Misuse Act* (June 2004), paras 100-107.
69. Law Com. No.186, *Computer Misuse.* Cm.819 (1989), para.2.23.
70. Law Com. No.186, *Computer Misuse.* Cm.819 (1989), paras 2.24-2.25.
71. B. Napier, " Update on the CMA 1990" [1994] J.B.L. 522, 527.
72. See, e.g. A. Flanagan, " The Law and Computer Crime: Reading the Script of Reform" (2005) 13 I.J.L. & I.T. 98.
73. APIG Report, *Revision of the Computer Misuse Act* (June 2004), para.89.
74. Examples include the *Melissa Virus* (1999), the *Sobig F Virus* (2003) and the *SasserWorm* (2004).
75. See, e.g. APIG Report, *Revision of the Computer Misuse Act* (June 2004), para.91.
76. M. Wasik, *Crime and the Computer* (1991), p.66.
77. See, generally, D. Miers, *Responses to Victimisation* (1978).
78. See, generally, H. Edelhertz, *The Nature, Impact and Prosecution of White-Collar Crime* (1970).
79. L. Lessig, *Code and other laws of cyberspace* (1999), p.123.
80. Wilding, " Hacked Off" (2006) 156 N.L.J. 753.
81. Wilding, " Hacked Off" (2006) 156 N.L.J. 753.
82. D.S. Wall, " What are Cybercrimes?" (2005) 58 *Criminal Justice Matters* 20.
83. Through its 10 point Action Plan for Combating " Hi-Tech Crime' --see *http://news. bbc.co.uk/1/hi/sci/tech/38671.stm* [Accessed September 21, 2008].
84. Through its Convention on Cybercrime-- see *http://www.conventions.coe.int/Treaty/en/Treaties/Html/185.htm* [Accessed September 21, 2008].
85. Through its Framework Decision 2005/222/JHA on attacks against information systems--see *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:EN: HTML* [Accessed September 21, 2008].
86. The maximum term of imprisonment on summary conviction has been raised to 12 months, and been set at 2 years on indictment--see the new s.1(3) of the CMA 1990, as amended by s.35 of the PJA 2006. However, at the time of writing (October 2008), s.154(1) of the Criminal Justice Act 2003 has not yet come into force. This renders later, statutory references to 12 months' maximum sentences in the magistrates' courts (such as this one in the amended CMA) ineffective. Consequently, for now, the maximum term of imprisonment on summary conviction for ss.1, 2 ,3 and 3A CMA offences remains at six months--see s.38(6) of the PJA 2006.
87. Art.6.
88. See *http://www.conventions.coe.int/Treaty/en/Treaties/Html/185.htm* [Accessed September 21, 2008]
89. See *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:EN:HTML* [Accessed September 21, 2008].
90. Which can be temporary--s.3(3)(c).
91. Walden, *Computer Crimes and Digital Investigations* (2007), p.181.
92. See Art.5.
93. See Art.3.
94. See the new CMA s.3(3), as inserted by PJA 2006 s.36.
95. As inserted by PJA 2006 s.37.
96. APIG Report, *Revision of the Computer Misuse Act* (June 2004).
97. APIG Report, *Revision of the Computer Misuse Act* (June 2004), para.75.
98. S. Fafinski, " Hacked Off" (2006) 150 S.J. 560, 561.
99. See s.3A.
100. See Art.6.
101. Including software--s.3A(3).
102. APIG Report, *Revision of the Computer Misuse Act* (June 2004).
103. Ethical hackers who seek, and then expose, computer and network security weaknesses.
104. Walden, *Computer Crimes and Digital Investigations* (2007), p.196.
105. *Hansard,* HC Standing Committee D, col.262 (March 28, 2006).
106. *Hansard,* HC Standing Committee D, col.267 (March 28, 2006).
107. Quoted from a Home Office letter by the Earl of Northesk; see *Hansard,* HL Vol.684, col.612 (July 11, 2006).
108. *Hansard,* HL Vol.685, col.213 (October 10, 2006).
109. *Hansard,* HL Vol.684, col.611 (July 11, 2006).
110. See, e.g. the recent hack into a US governmental email system--" Cyber attack on Pentagon email" , *BBC News,* June 22, 2007--*http://news.bbc.co.uk/1/hi/world/americas/6229188.stm* [Accessed September 21, 2008].
111. See D.S. Wall, *Cybercrime: The Transformation of Crime in the Information Age* (2007), p.47.
112. Potent, malicious software in the form of meta-trojans which contain many layers of viral infection.
113. The other three being " code" , markets and norms.
114. See generally, L. Lessig, *CODE and other laws of cyberspace* (1999).
115. L. Lessig, " The Law of the Horse: What Cyberlaw Might Teach" (1999) 113 *Harvard Law Review* 501, 546.
116. See, e.g. J.P. Barlow, " Thinking Locally, Acting Globally" *Cyber-Rights Electronic List,* January 15, 1996; see also J. Wallace and M. Mangan, *Sex, Laws and Cyberspace* (1996).
117. See generally, J. Goldsmith and T. Wu, *Who Controls the Internet? Illusions of a Borderless World* (2006).
118. Goldsmith and Wu, *Who Controls the Internet?* (2006), p.164.
119. See, generally, D.S. Wall, " Maintaining order and law on the Internet" in D.S. Wall (ed.), *Crime and the Internet* (2001).
120. The new ss.3 and 3A of the CMA.