HACKING AND COMPUTER VIRUSES -- the legal dimension

Matthew K. O. Lee †

1. Introduction

Computers permeate every aspect of modern life and commerce. They have found extensive use in both the public and the private sectors: e.g. air traffic control systems, hospital systems for administering drugs, weapon defence systems, automatic stock control, modern fly-by-wire aircrafts, robotic control of machines and manufacturing processes, issuing of pay cheques, automatic share trading systems, and so on. Apart from their traditional use as a sophisticated means of information storage/retrieval computers are used increasingly to make decisions and trusted to control important operations themselves without human supervision. Obviously, the potential for mischief is enormous if such systems are tempered with illicidy.

Illicit tempering of computer systems (generally termed as computer misuse) takes many forms the most common of which are probably hacking and computer viruses. Hacking generally refers to activity of gaining unauthorized access to a computer system (or network etc.). Computer viruses generally refer to programs which replicate themselves, delete stored information from the infected computer, or alter the information stored therein etc. thereby impairing the normal usage of the computer system in question. Hacking is often the first step in a computer misuse instance. Once a hacker has managed to gain unauthorized entry to a computer system he or she can then try to reprogram the system, delete or modify the data contained therein, or indeed infect the system with computer viruses etc. with grievous consequences. Actual reported cases include the hacking and illicit reprogramming of a computer controlled robotic manufacturing system by a disaffected employee, resulting in the machine reacting unpredictably to commands and thus almost killing a shop-floor operator; a hacker obtaining illicit access to a tour operator's computerized reservation system, swamping it with false orders and causing great havoc; the self-styled "mad hacker" who obtained illicit entry into a national computer network and subsequently infected the computers therein with a self-replicating program (i.e. a computer virus) causing the network to overload and eventually grind to a complete halt. Over 270 cases of computer misuse of one kind or another have been recorded by the DTI during the past 5 years. Only 6 cases out of the 270 actually ended up in court and convictions were secured in merely 3 of them. Indeed, knowledge of hacking is becoming widespread and is facilitated by, *inter alia*, the publicity it generates and the availability of electronic "bulletin boards" through which detailed hacking information is regularly disseminated among hackers all over the developed world. Open system architectures and inter-networking are now gaining widespread popularity but by their very nature they are even more prone to computer misuse such as hacking. The threat posed by computer misuse is indeed real and escalating. The essence of this threat is not so much about the inadvertent damage caused by computer misuse to the system concerned or the misappropriation of intangible property like information (which is generally not protected by the criminal law anyway), but the damaging effect on the integrity of the system concerned. If the general integrity of computer systems is in doubt, the willingness to invest in such systems may well dwindle and the effective use of them will be substantially impeded.

The threat posed by computer misuse can be countered by security measures and legal measures (which provides a deterrence against such a threat). Security measures are expensive to

† Dr. Lee is a barrister with BP International Ltd., IT Research Unit, BP Sunbury Research Centre, Chertsey Road, Sunbury-on-Thames, Middlesex TW16 7LN, email: matthew@bprcsitu.uucp

Authorized licensed use limited to: A.P.S. College of Engineering. Downloaded on March 10,2010 at 12:10:35 EST from IEEE Xplore. Restrictions apply.

implement and invariably inconvenience the users. Legal deterrences (in the form of relevant legislation) are relatively low-cost but their effectiveness depends on many factors (such as good drafting and successful prosecutions) which cannot be predicted accurately in the short term. Nonetheless, there is little doubt that in order to counter this threat effectively both security measures and legal measures should be relied on together and neither one of them alone is sufficient. However, the present state of development in computer security is far more advanced than the law in this area.

2. Legal Issues arising from Hacking and Computer Viruses

Hacking *per se* was never a criminal offence until 29th August 1990 when the Computer Misuse Act 1990 became operative. The criminal law does not generally protect confidentiality or privacy, or indeed provide sanctions against the removal or modification of private information. The idea of property in the criminal law does not generally extend to intangible property such as information. In cases involving dishonesty and the misappropriation of tangible property such as money the Theft Acts still apply and convictions have in fact been obtained even though the manipulation of computers is involved in carrying out the crime (e.g. fraudulent computerized transfer of funds to a false account). The real problem lies with the "innocent" hackers who may not have any criminal intent originally but once they have gained access to a system they may go on to commit fraud or cause damages, either by accident or design. Furthermore, the activities of some "innocent" hackers may serve merely as a smokescreen concealing people with more sinister ulterior motives. For instance, an apparently "innocent" hacker may try to hack into a banking computer system in order to commit fraud at some other time. However, before the fraud in question is actually committed it is unlikely that he or she can be convicted of *attempting* to commit fraud. For an offence of criminal attempt to be successfully made out the Criminal Attempts Act 1981 provides that an act must be done which is more than merely preparatory to the commission of the crime in question. Hacking into a computer system is only preparatory to the commission of the fraud in question and as such a charge of attempted fraud cannot be made out.

Another major problem area is computer viruses. Computer viruses often cause damage through the wiping out or alteration of useful programs and data stored in the infected computer, or simply through the using up of all the processing or storage capacity of the infected computer so that it cannot do anything useful. As far as damage is concerned, only property of a tangible nature is covered by the scope of the Criminal Damage Act 1971 (section 10(1)) although in the case of *Cox v Riley* [(1986)Cr App R54] the defendant deliberately erased a computer program from a circuit card of a computerised saw and was convicted of criminal damage. The circuit card was regarded as a tangible property which had been damaged because its value fell as a result of the program contained therein being erased. However, future convictions on similar grounds would be by no means certain and would very much depend on the interpretation of the word "damage" in each case. In fact it could be properly argued that the real damage occurred to the *intangible information* held by the storage medium (i.e. the circuit card) and not the physical storage medium *per se* and as such it was probably wrong to apply the 1971 Act. In any case the literal interpretation of the word "damage" necessitates some kind of *physical injury* to things. This state of affairs has created a level of uncertainty which is quite unacceptable in the criminal law context. One possible way to deal with this problem would be to amend the Criminal Damage Act 1971 to specifically include damage to computer material such as information held in computer memory. However, the mode of trial (i.e. summary or by indictment) with regard to offences under the Criminal Damage Act 1971 depends on the value of damage in question. It is particularly difficult to assess precisely and consistently the amount of damage to information in financial terms in every case. The resulting uncertainty in the mode of trial and consequently the severity of penalty is quite unacceptable. In any event it would be undesirable to muddle with the whole basis (i.e. damage to physical property) on which the 1971 Act was created just to accommodate this problem ad hoc.

Authorized licensed use limited to: A.P.S. College of Engineering. Downloaded on March 10,2010 at 12:10:35 EST from IEEE Xplore. Restrictions apply.

3. The Computer Misuse Act 1990

The Act (which came into effect on 29th August 1990) creates three new criminal offences with an increasing degree of gravity designed to tackle the problem of hacking and unauthorized modification of computer material in general (and computer viruses in particular). The new offences are as follows:

(1) Unauthorized access to computer material (the basic hacking offence).

(2) The same as (1) but with ulterior intent to commit or facilitate the commission of further offences (the ulterior intent offence).

(3) Unauthorized modification of computer material with intent to cause impairment.

The basic hacking offence has a very wide scope which covers almost all conceivable forms of unauthorized access to computer material which is taken as programs or data held in any computer. Access requires interaction with a computer by causing it to perform some function. Mere physical access to a computer is not enough. Access to programs or data is defined widely as any act of using, altering, erasing, copying, moving or outputting them (e.g. displaying them on screen). Unauthorized access means someone else is *entitled* to control access of the kind in question and the accessor in question does not have the requisite consent of access from that person who is *so entitled*. This offence certainly covers the "innocent" hackers who seeks access purely out of curiosity, or for the excitement and challenge of breaking into computer security systems. It also covers the act of testing the defences of a computer (i.e. knocking on the door) even though the hacker may not have managed to log himself or herself on to any computer at all. The act of trying to log on (e.g. by guessing password) constitutes access to computer material in the sense that the program for checking password is being used (i.e. executed). However, to be convicted of this offence the prosecution must prove that the hacker *knows* that his access is unauthorized at the time of access. This basic offence is triable summarily and carries a maximum of 6 months' jail sentence and/or a fine of up to two thousand pounds.

The ulterior intent offence is an aggravated form of the basic hacking offence accompanied by the ulterior motive of committing or facilitating the commission of any further offence carrying a maximum sentence of at least 5 years' imprisonment or for which the sentence is fixed by law (e.g. murder). This should cover most of the more serious offences under the Theft Acts (including fraud and blackmail) as well as the Offences against the Person Act (such as serious assault and manslaughter). It is immaterial whether the facts are that the commission of the further offence is impossible (analogous to the Criminal Attempts Act 1981). It is also immaterial whether the further offence is to be committed on the same occasion as the unauthorized access offence or on any future occasion. For instance, if a person hacks into a banking computer network in order to find out how he can (later when he wishes) illegally transfer funds into his own account then this ulterior intent offence can still be made out even though the act of hacking is *merely* preparatory to the commission of the intended offence of theft (and as such falls outside the ambit of the Criminal Attempts Act 1981). This aggravated form of the basic offence is triable either way carrying a maximum sentence of 5 years' imprisonment and/or an unlimited fine for conviction on indictment. On a charge of this ulterior intent offence an alternative verdict on the lesser offence of basic hacking is possible.

The third offence is directed against active interference with computer material. The offence is defined in terms of *any* intentional and unauthorized modification of the contents of *any* computer with the knowledge that such a modification is unauthorized. The requisite intent exists if the person in question intends to cause the modification and by so doing to impair the operation of *any* computer or to prevent, hinder the access to any program or data held in *any* computer, or impair the operation of *any* such program or the reliability of *any* such data. Any act that *contributes* causing any such modification is regarded as causing it. The generic use of the quantifier *any* means that it is immaterial whether the hacker knows the ultimate target computer or the actual form the

Authorized licensed use limited to: A.P.S. College of Engineering. Downloaded on March 10,2010 at 12:10:35 EST from IEEE Xplore. Restrictions apply.

modification takes. Further, the Act provides that it is immaterial whether the modification or the intended effect of it is permanent or merely temporary. As far as damage to intangible computer material is concerned, there is no longer any need to rely on (and face the uncertainty of) the Criminal Damage Act 1971 and prove that damage has been caused as a result of unauthorized modification to computer material (the act of unauthorized modification *per se* is sufficient). Indeed, the 1990 Act has provided that this type of conviction (based on non-physical damage to property) under the 1971 Act is no longer possible. The ambit of this offence is wide covering almost all presently conceivable forms of computer virus infection ranging from the direct addition of a virus to a computer's user library intending thereby to impair its operation simply by using up its capacity, to the putting into circulation of virus-infected floppy disks intending that the disks will cause deletion of data held on some computer somehow somewhere sometime. This offence is triable either way carrying a maximum sentence of 5 years' imprisonment and/or an unlimited fine for conviction on indictment. However, an alternative verdict on the lesser offence of basic hacking is possible.

Recognizing that computer misuse is often an international phenomenon, the other sections of the Act go on to deal with various trans-border modes of committing the offences, relevant jurisdiction, as well as various procedural matters. Two of the three new offences carry a maximum jail sentence of 5 years and as such they are *arrestable offences* within the context of the Police and Criminal Evidence Act 1984 (section 24(1)(b)). In a case where there is reasonable suspicion that an arrestable offence is being committed, the 1984 Act provides powers of arrest, entry in order to arrest, and search of the arrested person's premises. Although the basic hacking offence is not an arrestable offence, the 1990 Act has nonetheless specifically provided the power of entry to and search of any premises for relevant evidence (with a warrant issued by a circuit judge) on reasonable suspicion that a basic hacking offence has been or is about to be committed in those premises even though no arrest is made. So far as forfeiture of hacking equipment is concerned, the Criminal Justice Act 1988 (section 69(1)) has already provided adequate powers subjecting to forfeiture any property used or intended for use in committing offences. These are substantial weapons in enforcing the 1990 Act.

4. Conclusions

The annual cost of computer misuse to UK industry is estimated to be in excess of 400 million pounds currently. In cases involving direct fraud or theft the general criminal law is by and large effective in dealing with them. The 1990 Act will further fill some of the important gaps in the law exposed by alarming malpractices such as hacking and the spreading of computer viruses. The main purpose of the present Act is to provide a substantial deterrence against such malpractices which are seriously threatening the perceived integrity of computer systems. It is a clear indication that even "innocent" hacking can no longer be tolerated by society. However, it remains to be seen whether this deterrence will prove to be effective. In practice its effect will depend on how the Act is policed and interpretated and how many successful prosecutions are obtained. Terms used in the Act such as "computers" and "physical condition" etc. are not defined in the Act and remain to be interpreted by the courts. However, technically it is now quite feasible to detect and track down most cases of hacking. The power of entry and search without arrest conferred by this Act for even the basic hacking offence will no doubt further facilitate the policing of this Act.

Regardless of this Act, in the short to medium term UK industry is likely to continue to incur substantial costs in taking security steps against hacking and computer viruses. However, if the deterrence effect of this Act proves to be effective the equally substantial costs in monitoring and investigating hacking cases and taking corresponding remedial measures should be greatly reduced simply because there would be far fewer instances of such cases!

Authorized licensed use limited to: A.P.S. College of Engineering. Downloaded on March 10,2010 at 12:10:35 EST from IEEE Xplore. Restrictions apply.