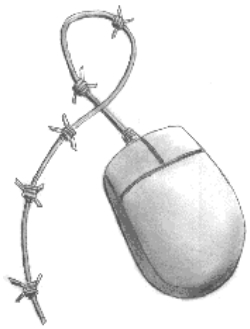
GreenNet IR Toolkit Briefing

Computer Crime



The law on the misuse of computers and networks

Written by Paul Mobbs for the
GreenNet *Civil Society Internet Rights Project*. Revision 1, April 2003.
http://www.internetrights.org.uk/

Computer crime is an oft-used term that has a very vague meaning. The law on computer crime tends to lag behind the actual practice of computer-based crime much more than is the case in other branches of crime.

Computers are a tool, and, like any other tool, can used by people intent on causing damage or carrying out some form of illegal activity. The nature of today's Internet and computer networks means that criminal activity can be carried out across national borders. This can create problems over the jurisdiction of those investigating the crime, and over differences in the law of the relevant countries where the crime took place; an activity deemed criminal in the home country of the target of the crime, for example, may not be considered so in the country from which the offending action was launched.

There are number of ways in which computers can be used for crime:

- to commit "real-world" crimes, such as forgery, fraud or copyright piracy, just like any other technical device; these types of computer-enabled crime are not usually prosecuted using other relevant laws rather than computer crime law;
- to damage or modify other computerised systems; these are the types of activity that are usually prosecuted using computer crime legislation;
- used for activities that cannot be prosecuted but that skate around the edges of legality; to the frequent frustration of law makers and security consultants, these sorts of activity cannot be legislated against because they often employ everyday, lawful means on the Internet.

Computers and the Internet are complex, but they function on a very narrow set of technical principles. This provides great flexibility, but makes it very difficult to legislate against certain types of activity without affecting others.

Recent legislation for clamping down on computer-based crime has fallen into just this sort of trap. Provisions in the *Regulation of Investigatory Powers* (RIP) *Act 2000*[1] for mass-surveillance of certain computer networks, for example, means that many innocent people could be covered as part of efforts to control a very small minority of 'Net users.

Governments and security organisations have in the past traded on the general lack of understanding of computers and the Internet to justify a more repressive approach to regulating the Internet, on very flimsy evidence. Examples of this are:

- The Parliamentary debate on the *Computer Misuse Act 1990*[2] - this debate was extremely

[1] *Regulation of Investigatory Powers Act 2000* - http://www.legislation.hmso.gov.uk/acts/acts2000/20000023.htm
[2] See Hansard, 9th February 1990.

alarmist, and mischaracterised the threats to online systems as well as the solutions to those threats. Much of the evidence advanced during the debate to justify the need for the Act (which was a Private Member's Bill introduced by Emma Nicholson MP) was poorly researched; a lot of it was merely scare stories promoted by certain sections of the media. It is arguable that at that time there was any need for computer misuse legislation at all.

- Recent justification for regulation to control the fraudulent use of credit cards on the Internet - credit card abuse on the Internet represents only 2% of all credit card fraud.[3] A wide variety of actions, such as logging all transactions on the Internet by all users, have been proposed to control this problem. 'Net-based credit card fraud is not as easy to carry out as other forms.

Clearly, such debates are not based on the facts of the threats involved. Many of the problems which cause disruption to computers, be it viruses or the cracking of online systems, are actually enabled by poor software.

We must therefore question whether it is more effective to introduce measures with serious civil liberties implications (such as the RIP Act) or require software producers such as Microsoft to plug the serious security holes in their computer software.

The following sections consider the current scope of the law in relation to computer and computer-enabled crime. The last section also looks ahead to the impact of future laws, such as the proposed Cybercrime Convention.

Computer-enabled crime

Computers enable crime - from the scanning of documents as part of a fraud, to the use of office software in managing the proceeds of crime.

Ordinary laws are currently used to prosecute five types of computer-enabled crime:

Fraud

As the Law Commission has noted, computer-enabled fraud is not new; it just takes "real world" frauds and uses the Internet as a means of reaching the victim.[4]

Computer-enabled fraud comes in many forms, from get-rich-quick schemes that don't exist, to emails that demand an additional fee to be paid by credit card via a web site to prevent losing Internet access. Most computer-enabled frauds are able to take place because:

- People do not understand how the technology works, and so are fooled into taking an action; or
- People put too much faith in the information they receive via their computer and so undertake actions that they would not ordinarily do in the real world.

Computer-enabled fraud, especially that using the Internet, is difficult to investigate. This is because many fraud-related sites are temporary - operating only for a few days before disappearing. Many frauds are enabled in one country but carried out in another, making it difficult for police to investigate.

[3] *Net Accounts for Only 3% of Credit Card Fraud*, The Guardian, Saturday June 23rd 2001. See http://www.guardian.co.uk/Archive/Article/0,4273,3952316,00.html

[4] Paragraph 8.42, Law Commission Consultation Paper No.155 - *Legislating the Criminal Code: Fraud and Deception*, March 1999 - http://www.lawcom.gov.uk/231.htm

In the UK, fraud is characterised as:[5]

> *A person who by any deception dishonestly obtains property belonging to another, with the intention of permanently depriving the other of it? For the purposes of this section 'deception' means any deception (whether deliberate or reckless) by words or conduct as to fact or as to law, including a deception as to the present intentions of the person using the deception or any other person.*

However, cases involving the use of machines, or the Internet, as part of deceptions,[6] have found that a deception, and hence fraud, cannot take place where a machine is manipulated by others to obtain a service (giving a false credit card number when signing-up for an online service, for example).

These means that it is unlawful for you to be defrauded by a computer-related system, but it is not unlawful for you to defraud a computer. The courts do not regard a machine to be "deceivable" because it is automated. The one exception to this is where the deception involves a licensed telecommunications service, such as dial-up chat lines or pay-per-view TV cards, in which case it would be an offence under section 42 of the *Telecommunications Act 1984*. The Law Commission[7] has recommended that new legislation should be drawn up to deal with this anomaly.

Another problem with the current law on fraud is that the courts have not recognised the information stored on computers as constituting "property". In a case involving the alteration of mortgage records,[8] and another of a student photocopying an exam paper and then replacing the original,[9] the courts chose to view the information contained in the records as being incidental to the physical property involved. This has implications for the use of information as part of "fraudulent" actions. In the former case, following the decision of the court the government had to rush through emergency legislation to introduce a new offence of "obtaining a money transfer by deception". But the general principle, that obtaining information, providing the original physical article had not been taken, is not unlawful, still applies.

Forgery

Forgery is the art of passing off a copy of something as the real article. Computers can be very useful for passing off documents as real - for example scanning a signature and then laser printing that signature onto another document, or scanning a driving license, altering the required information, and then printing out false driving license using a colour laser printer for use as bogus identities.

Computers are particularly able to forge digital information. This is because digital information can be copied and manipulated with very little evidence of alteration or replication having taken place.

Under UK law,[10]

> *A person is guilty of forgery if he makes a false instrument with the intention that he or another shall use it to induce somebody to accept it as genuine.*

The law on forgery can therefore encompass a whole variety of activities that can be enabled by computer. A "false instrument" could be a floppy disk, tape, sound track or other device upon which information is recorded, as well as documents, articles and images. Therefore the existing law adequately covers the

[5]Section 15, *The Theft Act 1968*.
[6]The *Clayman* case - see *Times Law Reports*, 1st July 1972.
[7]Law Commission Consultation Paper No.155 (see note 4 above).
[8]*R v Preddy* [1996] 3 All ER 481.
[9]*Oxford v Moss* [1978] 68 Cr App R 183.
[10]Section 1, *Forgery and Counterfeiting Act 1981*

common uses of computers for forgery and counterfeiting.

The only quirk in the current law exists because of a case[11] that came before the High Court before computer misuse legislation was enacted in the UK. The court decided that the passwords sent to a computer could not be considered forgeries since, in the same manner as fraud, it was not possible to ask a computer to determine the difference between a real article and a forgery. The case arose when someone gained access to BT's Prestel service and then to people's mailboxes. It has implications for circumstances where someone uses a forged identity (a copy of a machine-readable card, for example) in order to gain access to a location or online service, but where the use of the forged card does not constitute a fraud or computer misuse.

Obscenity and hate speech

Computer-based pornography and other images or material have been one of the main grounds of calls for greater regulation of the Internet. Current law, however, already covers the distribution of obscene images over the Internet, or by other forms of computer hardware such as disks or CDROMs.

Principle legislation covering computer-enabled obscene publications is:

- Section 43 of the *Telecommunications Act 1984*, which prohibits the sending of obscene material over public telephone networks; and
- The *Protection of Children Act 1978*, as amended by the *Criminal Justice Act 1988* and the *Criminal Justice and Public Order Act 1994*, on the creation or possession of child pornography.

The other "obscenity" that pervades computers is hate speech - for example, homophobic or racist material.

The UK law currently addresses racist material through section 17 to 28 of the *Public Order Act 1986*:

- Section 17 defines racial hatred as "hatred against a group of persons defined by reference to colour, race, nationality (including citizenship) or ethnic or national origins";
- Section 18 makes it a criminal offence to use "threatening, abusive or insulting words or behaviour" that express racial hatred. The term "words" also applies to the written word, but with the caveat that the intent of these words must be to incite racial hatred (this exists to differentiate hate speech from literary or dramatic material);
- Section 19 applies the above terms to the publishing of material that incites racial hatred; and
- Section 23 makes it an offence to possess material that incites racial hatred.

Currently there is no law that covers action or material that advocates hatred of homosexuality (either via computers or otherwise) unless such action amounts to threatening violence or constitutes a breach of the peace (which it is unlikely to do via computer).

Criminal damage

Prior to the implementation of the *Computer Misuse Act 1990*, damage to computer systems was prosecuted as criminal damage under the *Criminal Damage Act 1977*. Although a prosecution for criminal damage is unlikely, it is still possible where the case for "computer misuse" is tenuous. This might be where an employee deletes files from an employer's computer system as a means of retribution or revenge against the employer, for instance.

[11] *R v Gold* [1987] 3 WLR 803.

For a prosecution to succeed on the basis of criminal damage, it must be demonstrated that the system affected has been physically damaged. The law of criminal damage does not reflect the incidental value of the data on a computer system, only the computer system itself. So, for example, the deletion of an extremely valuable database is not criminal damage. On the other hand, a person causing the electrically programmable ROM BIOS chip (vital for the computer to function) erase itself, and rendering the computer useless, would be guilty of criminal damage.

Copyright

Most offences in relation to copyright are civil offences, and therefore require legal action to be instigated by the owner of the copyright that is being violated.

Certain industrial-scale operations, however, such as the bulk copying of computer software, can be prosecuted as a criminal offence under section 107 of the *Copyright, Designs and Patents Act 1988*[12].

The Computer Misuse Act 1990

The *Computer Misuse Act 1990*[13] covers certain offences specific to the penetration, alteration and damage to computer systems.

The law itself was drafted very generally, in the hope of ensuring enough scope so that the law would not date, as computer technology developed. However, this means that the Act can be rather a blunt instrument. If, for example, you changed the settings on your neighbour's computerised washing machine without permission, you would technically be in breach of section 3.

Computer crime also raises issues of data protection. Some actions involving computer crime, such as authorised access to data for unauthorised purposes (there have been some prosecutions of police officers who had access to the police national computer on this basis), then the Computer Misuse Act is not applicable. This is because the Act only considers "unauthorised access". However, it is possible for authorised access to a computer, for unauthorised purposes, to be prosecuted under the *Data Protection Act 1998*.

To understand the operation of the Computer Misuse Act it is necessary to consider the three main sections, according to their function. We look briefly at the Data Protection Act after that.

Cyber-trespass - section 1

Section 1 of the Act covers offences in relation to "unauthorised access". As noted above, there is a loophole in relation to those who have authorised access, and use it to undertake activities not covered by section 2 or 3 below.

"Access" itself is a broad term. As well as actual unauthorised access or logging onto a system, it could also encompass just turning a computer on. An offence under section 1 is punishable by a £20,000 fine or 6

[12] *Copyright, Designs and Patents Act 1988* - http://www.legislation.hmso.gov.uk/acts/acts1988/Ukpga_19880048_en_1.htm
[13] *Computer Misuse Act 1990* - http://www.legislation.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm

months imprisonment.

For an offence to be committed you must seek to access the computer in order to use or obtain access to the programs or data it holds. The first prosecution under section 1 of the Act (involving a former company employee who obtained a discount on goods by entering a command on computer when purchasing goods from the erstwhile employer's store) created a serious challenge to the Act. The court accepted the argument that the original drafting of the Act implied that two computers must be involved (such as an Internet-enabled hack attack on another computer, for example). For this reason the Government appealed the decision and had it overturned in the Court of Appeal.

An important aspect of section 1 is the matter of "intent". The section is drafted in such a way that *intention* to access a computer is all that matters. So if you try to access the computer, and fail, then you would still have committed an offence if your intent was to gain access. This creates a problem of proof for those using certain tools on local networks or the Internet for tracing information. For example, using a 'port scanning' program to probe the services available on a computer and whether or not they are working.

Some computer misuse legislation in other countries, such as the Norwegian Penal Code, requires that an attempt be made to pass or circumvent the security measures installed on the system. Indeed, during the passage of the UK Bill there was a proposed amendment to section 1, requiring that it only be used for prosecution where the computer's operators had put measures in place to prevent access. This amendment was defeated.

This section of the act clearly raises the issue of someone innocently stumbling into an unsecured area of a computer/web site, and obtaining or viewing information; Under the current drafting of section 1, the owner of the system could successfully prosecute on the grounds of unauthorised access.

Cyber-theft - section 2

Section 2 of the Act deals with the objectives of unauthorised access.

Many professional hackers do not crack the security of a particular computer with the intent of accessing the information on that computer. Instead, they use that computer as a base, or *zombie*, from which to carry out attacks on other systems. In this way they can remain one step removed from the computer that they are targeting.

Section 2 covers offences where access is secured to a computer for the commission of a 'relevant offence' (that is, any crime for which the penalty is fixed by law, or which carries a prison term of five years or more), and on conviction carries a sentence of five years' imprisonment.

As with section 1, the section is drafted in such a way that it is the *intent* that matters, not whether the offence was possible.

For example, if you penetrated a bank's computer system intending to move £10,000 to another account, you would still be guilty of an offence under section 2 even if doing so was actually impossible (because of the configuration of the system).

The drafting of this section also means that the offence need not be committed on a particular occasion. Therefore if someone penetrated a computer with the intention of setting up an account to access the site in the future for some sort of fraud, they would be committing an offence under section 2 even if they never returned to commit the offence.

Under sections 1 and 2, a prosecution can also be on the basis of a conspiracy. For example, if someone

penetrated a computer to obtain the identity keys for a number of mobile phones; gave or made available that information to someone else; and that person used it to reprogram mobile phones to obtain calls on someone else's bill - then the person would be guilty not only of unauthorised access under section 1, but also of conspiracy for theft or fraud under section 2.

Cyber-violence and Malware - section 3

Cyber-violence is a general term to describe the wrecking, wiping or deletion of information from a computer system. *Malware* (i.e., software that causes you harm) usually relates to computer viruses, worms or Trojans which may cause similar damage.

Section 3 covers offences where, having accessed a system, either in person or through the guise of a computer virus or some other automated means, a person modifies the computer system in a manner that "impairs" its operation. Section 3 carries a sentence of up to five years' imprisonment.

Once again, the drafting of the law in this section is on the basis of intent. Therefore, if someone writes a computer virus with the intent of releasing it to others, they are guilty of an offence at the moment of release, rather than when, or even if, it successfully infects a computer system.

Software program writers need to take careful account of section 3. It means that software should not be designed to delete anything without the express consent or authorisation of the computer's user.

An early prosecution under this section was that of a software writer who distributed software for free; if the user wished to use the programme they had to be licensed for the software within 30 days, or else the program deleted itself. One user presumably complained about this, and the court decided that it constituted "unauthorised modification" under section 3 and the program writer was successfully prosecuted.

The Data Protection Act and unauthorised access to personal data

The Data Protection Act covers "unauthorised" access.

The limitations of the Computer Misuse Act were seen in the case of *DPP v Bignell*, where two serving police officers accessed the police national computer (for which they had authorisation) to obtain information for their personal use. The court decided that the Act protected the computer system as a functioning unit, but not the value of the data stored upon the system.

The *Data Protection Act 1998*[14] covers specific offences relating to the processing of data without the authorisation of the data subject, and to the unauthorised procurement of data. Although the operator of a data bureau would usually be responsible, section 61 of the Data Protection Act provides that a director, manager or similar officer can be found personally liable for any wilful or neglectful breach of the Act. Whilst access to the data on a system does not, therefore, constitute a crime under the Computer Misuse Act if it is carried out by an authorised person, it could be an offence if that data were personal data notifiable under the Data Protection Act.[15]

[14] *Data Protection Act 1998* - http://www.legislation.hmso.gov.uk/acts/acts1998/19980029.htm

[15] For a more detailed briefing on the workings of the Data Protection Act see the GreenNet IR Briefing no.2 on *Data Protection*

New laws for the 'Net

The above laws represent the framework of computer-related law in the UK until 2001. New laws are due to be enacted by early 2002 to take account of the need for a legislative framework for e-commerce and the Internet.

One of the Government's priorities in its first term was to update existing laws on surveillance and telecommunications. The result of this review, the *Regulation of Investigatory Powers Act* (RIP) *2000*,[16] introduced new powers for police and the state to intercept communications via the Internet, and enhanced existing powers to intercept telecommunications.

The RIP Act also created a number of new powers and offences with serious implications for civil rights on the Internet:

- Under the heading of *the maintenance of interception capabilities*, the Government, backed up by the courts if necessary, can force an Internet service provider to copy some or all of their traffic, redirecting it to a new computing centre being developed by the security services (MI5). The purpose of this is to aid the collection of *traffic data* (used to map the movement of communications between persons on the 'Net) and to allow the surveillance of groups or individuals. There is also a proposal to store this information for between four and seven years.
- The Act creates powers whereby people who hold encryption keys may be forced to disclose them or else face prosecution. It includes a clause which provides that such a person may be prohibited from informing anyone else that they have been served with notice to disclose a key.

The real impact of this legislation remains to be seen, and we will have to wait a few years to see how it affects the operations of Internet service providers and those who are investigated under the Act.

Future developments in legislation

There have been a number of proposals in recent years for some form of international co-operation on computer crime. These have often been made on the basis of economic rather than crime concerns, by groups such as the Organisation for Economic Co-operation and Development (OECD).

Efforts have been made to establish increased co-operation on the use of extradition, and to deal with questions of jurisdiction within that. This does not solve the problem of variation and incompatibility between states' legal codes, however, and there is still no internationally agreed definition of computer crime.

The European Union has made some progress on a co-ordinated approach to computer crime. The Treaty of Rome did not cover police and security activities, but with the Maastricht Treaty the work of the European Union has extended to a new 'Third Pillar' of home affairs and justice. This has spawned a new European project, ENFOPOL[17], part of which involves setting standards for the monitoring and investigation of computer crime[18].

The new Cybercrime Convention[19] covers the same types of issues outlined earlier - computer intrusion,

[16] *Regulation of Investigatory Powers Act 2000* - http://www.legislation.hmso.gov.uk/acts/acts2000/20000023.htm
[17] The purpose of ENFOPOL is specified in a written answer in the Journal of the European Communities [C 13.32 EN 18.1.1999 - 1999/C 13/043] - http://www.heise.de/tp/english/special/enfo/6389/1.html
[18] For information on the ENFOPOL process see http://www.heise.de/tp/english/special/enfo/
[19] Cybercrime Convention - http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185&CM=1

forgery, copyright and pornography. It also extends the current law. Its definition of offences related to "aiding and abetting" other offences covered in the treaty has implications far beyond existing conspiracy laws in the UK. It formalises the procedure for the search and seizure of computers (much like the FBI's current policy in the USA). The treaty also incorporates many of the features of the *Regulation of Investigatory Powers* (RIP) *Act 2000* [20] in relation to forcing the disclosure of decryption keys. The treaty also incorporates UK proposals for the monitoring of networks, under proposals for the acquisition and storage of *traffic data*. Information gathered will be available for exchange between all the national governments signing up to the treaty, potentially creating a seamless web of surveillance of activities using electronic networks across Europe.

The development of the treaty, in the face of opposition from many groups across Europe, will define, to some extent, how the Internet will be used by groups actively working for change - particularly those who use the Internet to organise protest actions. The experience of the interpretation and development of the RIP Act in the UK is a valuable indicator of what we may expect.

Further work

This briefing has been written in the context of the legal framework currently in force in the UK. If you live outside the UK you will need to make yourself aware of the procedures operating in your own country. Key points you will need to find out are:

- Does your state have specific laws on computer misuse?
- Do data protection laws define forms of computer misuse?
- Are there other aspects of the law, particularly in relation to sexual material, racial harassment or defamation that apply additional legal sanctions for the misuse of computers and computer networks;
- Have there been any significant prosecutions of computer hackers which have defined how systems for tracking and prosecuting computer misuse works?
- Does your state intend to adopt the proposals contained in the Cybercrime Convention?

You should also contact any civil liberties organisations operating in your country. They may be able to provide you with much of the information you need computer misuse.

The GreenNet Internet Rights Project

GreenNet[21] is the UK member of the Association for Progressive Communications[22] (APC), and is leading the European section of the APC's Civil Society Internet Rights Project[23]. The primary goal of this project is to provide the resources and tools necessary to defend and expand space and opportunities for social campaigning work on the Internet against the emerging threats to civil society's use of the 'Net. This involves developing ways and means of defending threatened material and campaigning, as well as lobbying to ensure a favourable legal situation for free expression on issues of public interest.

[20] For more information on the RIP Act see the GreenNet IR Toolkit Briefing no.13 on *Interception Capabilities* and no.3 on *Encryption and Digital Signatures*
[21] GreenNet - http://www.gn.apc.org/
[22] APC - http://www.apc.org/
[23] CSIR Project - http://rights.apc.org/

Until recently, the social norms of Internet communities, together with a very open architecture based on supporting these norms, regulated the Internet, and was responsible for its openness. The main forces of regulation now, however, are the business sector and government legislation. Corporations and governments are pressing for fundamental changes in legislation and in the architecture of the Internet. Unless challenged, these moves could radically change the nature of the 'Net, making it a place of oppressive controls instead of freedom and openness. It is in this context that APC's Internet Rights project is being developed.

This briefing is one in a series[24] that document different aspects of work and communication across the Internet. Although written from the perspective of the UK, much of its content is applicable to other parts of Europe. There is continuing work on these issues, as part of the European project. If you wish to know more about these briefings, or the European section of the APC Civil Society Internet Rights Project, you should contact GreenNet. You should also check the APC's web site to see if there is already a national APC member in your country who may be able to provide local help, or with whom you may be able to work to develop Internet rights resources for your own country.

[24] http://www.gn.apc.org/action/csir/index.html#briefing

