Police Powers to Hack: current UK law

Peter Sommer

Law enforcement power to intrude into computers associated with suspects would seem, from the perspective of those carrying out investigations, highly desirable. What are the actual powers and current limitations?

On 5 January 2009 many UK papers and media outlets ran a story saying that the police had been given powers to hack into personal computers without a warrant. The stimulus was a comment from the Home Office reacting to a European Parliament Council of Ministers plan of 27 November 2008 to strengthen the fight against cybercrime and to lay the way open for cross-border co-operation.[i] The implication was that these UK powers were new and that "warrantless" meant they could be used at will provided that a Chief Constable or equivalent thought that the deployment was necessary and proportionate.

The position is rather more complicated. Nearly all of the law has been in place for many years and does require a significant level of "authorisation". However it seems some aspects will need updating. We need to look at the underlying technologies available, the empowering laws, issues of disclosure and the risks that contamination of evidence in the course of acquisition may render potential exhibits or expose law enforcement to rigorous cross-examination. A further consideration from the perspective of law enforcement is the ability to carry out surveillance without alerting the target. However it turns out that the use of many of the technologies is easily detected, thus reducing their value and indeed imperilling investigations.

For the purposes of this article we will look both at law enforcement intrusions into personal computers of interest and at obtaining access to password-protected computer servers on the Internet. Although the law discussed is specific to England and Wales, a number of the issues are generic to designing any workable framework for regulating law enforcement intrusion into suspects' computers.

Contamination: ACPO Good Practice Guide

There is a practical problem which runs through all forensic examination of computers and digital evidence, and that is particularly true of "hacking" methods: the activity of examination will often cause the data being scrutinised to be altered, or as a defence lawyer or expert will say, contaminated. When a computer is started up, data is being written to the hard disk and also when it is being closed down even if the user has done no more than look briefly at the display. Log files are written to when some-one signs in, file time-and-date stamps are being altered as programs are started up and files viewed even if the user makes no conscious alteration. Some programs create temporary "workspace" files. Other alterations may take place in hidden parts of the operating system, the registry, for example, or the facilities which are being created in background to be able to recover from a fault or crash.

Once it is known that law enforcement have carried out live intrusion of a computer, it is very likely that defendants will claim that officers have imported or altered data artificially to strengthen their case.

To meet the challenges of contamination the Association of Chief Police Officers has a Good Practice Guide, first issued in 1998 and about to appear in a fifth edition[ii]. It isn't law nor is it a statutory Code of Practice, but breach will result in the drawing of adverse inferences. The Principles say:

> Principle 1: No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.
> Principle 2: In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
> Principle 3: An audit trail or other record of all processes applied to computer based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
> Principle 4: The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

The gold standard for means of adherence is to remove the hard disk from its computer, mount it in "write-protect" hardware (to stop any writing of data to the disk in question) and then the deployment of forensic imaging software to make a complete image copy of the hard disk including sectors which appear to be empty. The image can then be analysed – and that includes the possibilities of recovering deleted data and examining normally-hidden parts of the disk, The same set-up can be used to carry out an initial preview to see if a disk contains anything of interest before the full forensic image is made.

It is also possible to use specialist CDs and USB thumb drives which contain an independent operating system which boot up the computer running and feature disk examination tools; there are software facilities to stop writing to the disk being examined. Forensic disk imaging is seldom possible in a live police "hacking" situation.

The Good Practice Guide allows law enforcement officers to carry out direct examinations[iii], but usually only on the basis of operational necessity and with provision of a full audit trail. As we will see, "hacking" methods nearly always involve direct examination.

The Technologies

Quite subtle changes in the *modus operandi* of the "hacking" method can have radically different outcomes in terms of legal impact.

Law enforcement officer has direct physical access to computer and enters it

This is the simplest of all situations. The legal position here is that the officer has explicit protection under s 10 Computer Misuse Act, 1900 (CMA):

> 10 Saving for certain law enforcement powers.
>
> > Section 1(1) above has effect without prejudice to the operation—
> > (a)in England and Wales of any enactment relating to powers of inspection, search or seizure; and
> > (b)in Scotland of any enactment or rule of law relating to powers of examination, search or seizure.
> > and nothing designed to indicate a withholding of consent to access to any program or data from persons as enforcement officers shall have effect to make access unauthorised for the purposes of the said section 1(1).In this section "enforcement officer" means a constable or other person charged with the duty of investigating offences; and withholding consent from a person "as" an enforcement officer of any description includes the operation, by the person entitled to control access, of rules whereby enforcement officers of that description are, as such, disqualified from membership of a class of persons who are authorised to have access

Section 1(1) of CMA is the offence of unauthorised access to a computer.

If the computer is password-protected and its owner or regular user is available, the officer can require access under s 20 Police and Criminal Evidence Act, 1984 (PACE):

> 20 Extension of powers of seizure to computerised information.
>
> > (1)Every power of seizure which is conferred by an enactment to which this section applies on a constable who has entered premises in the exercise of a power conferred by an enactment shall be construed as including a power to require any information stored in any electronic form contained in a computer and accessible from the premises to be produced in a form in which it can be taken away and in which it is visible and legible or from which it can readily be produced in a visible and legible form

If the computer or part thereof (or media containing data) is encrypted there are powers to issue a notice to compel decryption under Part III of the Regulation of Investigatory Powers Act, 2000 (RIPA): Section 49 sets out the circumstances in which a notice to disclose a decryption key or to provide material in unencrypted form can be issued. The grounds are: (a) in the interests of national security; (b) for the purpose of preventing or detecting crime; or (c) in the interests of the economic well-being of the United Kingdom. The notice must be in writing, must be signed by an identified senior officer and must pass several tests: that it has not been practical to obtain the suspected information in any other way, that it is necessary to do so and that the demand is proportionate to the overall threat. There is a detailed Code of Practice[iv].

Refusal to comply is a criminal offence with a maximum penalty of two years or five years if it involves national security or child indecency. The court would need to be convinced that the material is indeed encrypted that the accused does actually have the means of decrypting it and that the procedures laid down in the Act and Code of Practice have been followed.

Law enforcement officer has access via the Internet to a computer which is offering a public service, for example a web-server or a file-server.

Case 1: the service is not password protected. As the service is available to the public, law enforcement officers can view freely without the need for any separate warrant or authority

Case 2: the service is password protected. If the law enforcement officer has acquired the password through legitimate means, for example by asking for it, locating a piece of paper or a file with it, or guessing it, the officer's examination is protected by s 10 CMA. There may be some defence query about how the password was acquired and objection raised if the method involved some further breach of law or absence of proper warrant or authorisation. We will consider some of these "illegitimate" or questionable means of password acquisition later.

Case 3: there is a public service but the officer is able to "get behind it" by technical means and examine parts of a computer that the user intended to keep private Everything depends on the precise technical means. One class of techniques is called "browser injection" – it consists of typing instructions into the place where you would normally input the name of a website you wished to visit. The effects can vary and exploit poor configuration on the part of the person who set up the computer: a SQL injection may result in disgorging an entire back-end database, a directory transversal or a buffer overflow may give the "hacker" full access to the entire computer. All of these activities amount to "unauthorised access", the s 1 CMA offence, for which the law enforcement officer has the protection of s 10 CMA.

Case 4: The investigating officer is able to get remote "shell" or "terminal" access to a computer and execute commands This is another instance where a computer has been badly configured and a hacker (or law enforcement officer) is able to get access. Shell access means the ability to issue commands (usually in Unix of a variant) and is the way in which geeks have traditionally run computers. Again this is an instance of a s 1 CMA offence with the law enforcement officer having the protection of s 10 CMA.

The position is little different if the shell asks for a username and password; provided the officer's means of acquiring the credentials is not *ultra vires* , the s 10 protection remains.

However s 10 only applies to actions which would otherwise be offences under s 1 CMA. Some hacking activities will involve a breach of s 3 CMA:

> 3 Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.
>
> (1)A person is guilty of an offence if—
> (a) he does any unauthorised act in relation to a computer;
> (b) at the time when he does the act he knows that it is unauthorised; and
> (c) either subsection (2) or subsection (3) below applies.
> (2)This subsection applies if the person intends by doing the act—
> (a) to impair the operation of any computer;

(b)to prevent or hinder access to any program or data held in any computer;
(c) to impair the operation of any such program or the reliability of any such data; or
(d) to enable any of the things mentioned in paragraphs (a) to (c) above to be done.

(3)This subsection applies if the person is reckless as to whether the act will do any of the things mentioned in paragraphs (a) to (d) of subsection (2) above.

(4)The intention referred to in subsection (2) above, or the recklessness referred to in subsection (3) above, need not relate to—
(a) any particular computer;
(b any particular program or data; or
(c) a program or data of any particular kind.

(5)In this section—
(a) a reference to doing an act includes a reference to causing an act to be done;
(b)" act" includes a series of acts;
(c) a reference to impairing, preventing or hindering something includes a reference to doing so temporarily.

We need also to look at the CMA's "interpretation" section, s 17, and in particular:

(2) A person secures access to any program or data held in a computer if by causing a computer to perform any function he—
(a) alters or erases the program or data;
(b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;
(c) uses it; or
(d) has it output from the computer in which it is held (whether by having it displayed or in any other manner);

S 17(2)(c) "uses it" is particularly wide.

And it this section 3 CMA offence which is engaged in the techniques most widely discussed in terms of "police powers to hack".

Back-door server control

The next situation to look at, and it is what is often thought to be the classic form of law enforcement "hacking", is where a computer is connected to the Internet but is not offering an obvious portal in. One has to be created by installing a "back door".

If you have Windows XP or later you already have at least one version of this on your computer, in the form of Remote Desktop. From your own machine you can log into a remote one and from then on your monitor shows the remote computer while your keyboard and mouse issue commands to run programs, display folders, and so on. There are two legitimate usages: to allow some-one control of their computer when they are away from its regular physical location – in an office or home, for example – and to provide remote assistance and support to people facing problems with their computers.

For this to happen the remote computer has a small server program which authenticates and admits you – and then accepts your commands. The server program is an intrinsic feature of XP Professional and nearly all versions of Vista and Windows 7. There are also commercial subscription services such as Logmein and

GotomyPC which offer enhanced functionality for cross-Internet connections – and which make it easier for PCs using dynamic IP addressing and behind NAT[v] routers to be easily located. (These are common situations for PCs attached to home and small business networks).

All these facilities have two components – the server program which is installed on the computer to be controlled and the client program which runs on the computer that does the controlling. In these very ordinary situations, the programs usually alert local users as to what is happening, and the server program is enabled or installed by the conscious action of the owner of the computer that is to be remotely controlled.

But there are also numerous hacker programs which perform the same or similar functions but which conceal their existence – there are no on-screen messages and some of them are sophisticated enough so that if the user calls up a screen to identify running processes (Task Manager - ctrl-alt-del in Windows), the program does not show up. These programs are usually called Trojans or Back Doors. The main challenge for the hacker is to get the server program installed without the knowledge of the computer owner. There are a large number of mechanisms to do this, but the most common are via email attachment or by clicking a link on a web-page. In both cases, the attachment or link look innocent but aren't – these mechanisms are also used to transmit viruses and web browser hijacks, and to set up the command-receipt function of botnets, in which large numbers of computers are remotely controlled and then told to send out masses of spam emails, or requests which overload a target computer whose owners will then be subjected to extortion.

Law enforcement *could* use these covert hacker programs and for all I know may have done so in the past. But they don't because more sophisticated facilities are available to them which allow much more elaborate and penetrating forms of analysis to be executed remotely. The best-known product is *Encase Field Intelligence Model* (http://www.guidancesoftware.com/products/fim_works.asp). The basic Encase product is widely used for "dead" static analyses of the contents of disks. The disks themselves are forensically imaged (that is, as we have seen, put through a process so that every sector on the disk whether occupied or not is copied and in a protocol which ensures the data remains unaltered and tamper-free). The EnCase analysis program is then able to present various "views" of the disk and its contents, recover deleted material, and carry out complex searches. For more details, go to http://www.guidancesoftware.com/products/ef_index.asp.
The Field Intelligence version can do all of these analyses remotely; moreover, since the computer is running, it can also inspect running processes and create snapshots of volatile data which might get lost if the computer were depowered. The website says that this version is only sold to law enforcement but there is another version – Enterprise – which is sold to businesses. This has the identical functionality, except that the servlet (Encase's name for the server program) is installed overtly by the organisation which owns the computers to be scrutinised; obviously there is less need for stealth than in the law enforcement/intelligence situation.

Other companies offer similar products.

The main *practical* weaknesses concern the dangers of easy detection. The server has to be installed on the target computer and it will look very like a Trojan, because that is what it is. As a result many of the common anti-virus programs are likely to react. (There are rumours that some A-V vendors have agreed not to include the signature of the servlet in their libraries, but this is certainly not true of all). Some A-V programs

have a "heuristics" function, where they work, not on signatures but on trying to detect the generic characteristics of malware. Even if a servlet is successfully installed, once it starts operating the traffic in and out of the targeted computer is likely to trigger any firewall that has been installed. Firewalls are usually initially configured to forbid or raise an alert about all programs. They ask the computer owner whether to "allow" programs to use various ports.

The law enforcement investigator using these stealth facilities thus faces the prospect that many attempts will fail because either anti-virus software or a firewall will thwart his ambitions. There is also a risk that if the owner of the targeted computer is curious about an apparent attempt at mounting a Trojan or why a firewall alarm has been set off, the investigator's interest in him may become known, leading the suspect to take further evasive action.

But there is also currently a substantive legal problem: the installation of the servlet or backdoor is a s 3 CMA offence in that it is more than unauthorised access and amounts to an impairment. Loss of believed confidentiality and security is a clear "impairment". As we have seen, s 10 CMA only protects law enforcement officers from a s 1(1) CMA offence.

Trojans and Backdoors can be detected , if suspected. Even if the author has taken trouble to conceal the files and processes which make the program work, in the end commands have to be sent from outside to get the programs to work and they, along with the data they send back to the remote controller can be detected as they pass in and out of the computer's Ethernet port onto the internet.

Physical Keyloggers

As the name implies, a keylogger captures the strokes imparted onto a keyboard. The aim may be simply to obtain username/password combinations, or to record entire sessions of activity. The two types of keylogger that exist further illustrate the problem that s 10 CMA does not protect against a s 3 CMA offence.

The first type is a physical device inserted between the keyboard and a computer, using either the PS/2 or USB connection, though there are modules which can be sued to install inside a keyboard.. It contains a chunk of memory which can later be retrieved on to an investigator's own computer. In pure investigative terms, the limitation is that it only captures what is actually typed and so excludes mouse movement and of course any on-screen reaction. Using this type of kit arguably does not involve any unauthorised access to a computer still less any "impairment". However unless the law enforcement officer can get legitimate physical access to the computer in order to install (and later retrieve it), there is the problem of a legal basis for arranging the installation covertly.

This will usually be on the basis of s 93, Police Act 1997, an authorisation to "interfere with property".[vi] As revised by the Regulation of Investigations Act, 2000 (RIPA):

> The action falling within this subsection is action for maintaining or retrieving any equipment, apparatus or device the placing or use of which in the relevant area has been authorised under this Part or Part II of the Regulation of Investigatory Powers Act 2000

Translated, this will also include audio and video bugs. The authorising officer is normally a chief constable or equivalent.

The *output* of the keylogger amounts to "surveillance" for the purposes of RIPA. This is covered in Part II of the Act. There are two sorts of surveillance: "directed" and "intrusive", the main difference being that intrusive surveillance is said to take place on residential premises or in a private vehicle, otherwise it is merely "directed" (s 26). Intrusive surveillance requires a higher level of authorisation.

We need to turn to s 48 to see what is meant by "residential premises" and s 26 (4) also says the surveillance is not intrusive if "it is surveillance consisting in any… interception of a communication". A physical keylogger installed in an office will this require authorisation for a "directed" not "intrusive" surveillance: S 28 RIPA as opposed to s 32, where the authorising officer is a chief constable or equivalent.

Thus two types of authorisation will be required, under s 93 Police Act, 1997 and under s 28 or s 32 of RIPA.

There is a risk to the investigator that their suspect carries out a detailed physical examination of their computers and discovers the keylogger, though most of them are physically very small.

Software Keyloggers

The second type of keylogger is software, nearly always covert. Although there are a number of variants, in addition to the actual keystrokes the products can also take still or moving screenshots of what the user is seeing; many products will covertly email or otherwise send the results to the person who installed them.

The practical problem is to arrange for the initial installation without alerting the user whose computer is being monitored. In effect routes very similar to those deployed for backdoor Trojans work very well.

The legal position is that the installation of is a s 3 CMA offence and with no current protection for law enforcement via s 10 CMA.

The problems of detecting software keyloggers are very similar to those for detecting back doors and Trojans.

RIPA Interception

There are other means by which a username/password can be acquired. One such is via monitoring traffic to and from a computer. There is nothing technically difficult about this; in its simplest form free software, Wireshark, can be downloaded from the

Internet and used in conjunction with a regular network card. The software can filter the traffic for words such as "username" and "password".

The legal position is that this activity is an interception for the purposes of Part I of RIPA, 2000. If the interception takes place on a *public* telecommunications service, an offence occurs unless a warrant has been issued; the warrant has to be provided by "the Secretary of State" which is for most purposes the Home Secretary of the day. There is also an offence if the interception takes place on a *private* system unless the interception is by or with the consent of the owner of the system. In the latter instance, even if there is no criminal liability there may be civil liability in terms of breach of privacy.

Employers should be able to have the benefit of the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. This allows a business to carry out an interception on its own network in order to: "establish the existence of facts", "in the interests of national security", "for the purpose of preventing or detecting crime", and "for the purpose of investigating or detecting the unauthorised use of that or any other telecommunication system".

Intercept evidence in the UK is currently inadmissible – s 17 RIPA: "no evidence shall be adduced, question asked, assertion or disclosure made or other thing done in, for the purposes of or in connection with any legal proceedings or Inquiries Act proceedings] which (in any manner)— (a) discloses, in circumstances from which its origin in anything falling within subsection (2) may be inferred, any of the contents of an intercepted communication or any related communications data; or (b) tends (apart from any such disclosure) to suggest that anything falling within subsection (2) has or may have occurred or be going to occur."

Thus law enforcement can successfully apply for a warrant to intercept and use the results as intelligence as opposed to evidence; and the defence is not entitled to know.

There are interesting consequences for the obligation of the prosecution to disclose, which we explore below. The specific guidance about handling requests for disclosure which might relate to interception requires a whole section in a CPS Guide[vii]: (The Crown Prosecution Service –CPS – is the body that frames criminal charges and brings cases to court)

WiFi interception

WiFi ethernet is now a very popular method for local area networking without the need for physical cables and instead uses radio. Most new-ish domestic and small office internet installations are based on a home hub device which contains a wi-fi access point[viii].

Many of these are "open", not encrypted, or have easily broken decryption[ix]. It is thus possible for an investigator to join the network and probe the attached machines for "shares"; with rather more difficulty, attempts can be made to monitor traffic on the local network.

The access point would almost certainly be regarded as a "computer" for the purposes of the Computer Misuse Act and of course there would be no doubt in respect of probed computers attached to the local area network. This then would be another instance where a law enforcement officer could claim the protection of s 10 CMA as only s 1 CMA offences would be involved.

A much more complex legal situation exists where another "wifi" route is attempted – the "evil twin"[x]. A rogue wifi hot-spot base station is set up in a public place close to where the target is using his computer. The rogue wifi hot-spot actually gives access to the Internet but also monitors traffic going through it. The typical aim would be to capture username/password combinations.

This would probably amount to "directed surveillance"[xi] in terms of setting up the monitoring facility, but the actual monitoring would almost certainly be an "interception" for the purposes of ss 1 and 2 RIPA, which would require a warrant signed by the Secretary of State; the results would fall within the admissibility restrictions of s 17 RIPA.

The scope of wifi hacks is limited to the physical range of wifi access points, usually under 100 meters.

Bluetooth Hacks

Bluetooth is a short-range wireless technology widely used in cellphones, smartphones and tablet. Many slightly-more-expensive laptops also have Bluetooth built-in. Because the technology is often not very securely implemented a number of exploits similar to Trojans on a personal computer exist – bluejacking, bluesnarfing, bluebugging and bluetoothing[xii]. Hacking software is widely available which is capable of acquiring data from the targeted device, including contact information, username/password combinations and substantive files.

As with the simpler form of wifi hacking, law enforcement officers would appear to be able to rely on the protection of s 10 CMA.

The scope of Bluetooth hacks is limited to the physical range of Bluetooth technology, usually within 10 meters.

Disclosure

The final element in the decision-making process of law enforcement officers contemplating the deployment of hacking techniques is disclosure.

In English criminal law, the prosecutor is under a continuing duty to disclose prosecution material not previously disclosed that might reasonably be considered capable of undermining the case for the prosecution against the defendant or of assisting the case for the defendant.[xiii] Ultimately a failure to disclose could result in a case being lost on the basis of abuse of process. Other sanctions can include an

order to exclude evidence from consideration at trial and the awarding of costs against the prosecution.

The CPIA regime also imposes a obligation on the defence to produce a defence case statement setting out the particular bases upon which it is intended to rely, including any issues of fact and any points of law. The defence can still go to court and argue that disclosure has been incomplete.

The general policy aim is to have trials where all the professionals, the judge and lawyers, know in advance what evidence is to be produced so that the trial consists of a clear and clean presentation to the jury (if there is one). The arrangement is in sharp contrast to most tv and film court-room dramas, where the stocks-in-trade are the last minute new witness and the just-discovered piece of vital evidence. Courts do not want either side to be ambushed.

Most of the detailed requirements in criminal disclosure are directed at law enforcement investigators and at prosecuting lawyers. The detail can be found in the Manual available on the website of the Crown Prosecution Service.[xiv]

Material which is collected by investigators in the course of an investigation but is not going to be used directly as evidence to support criminal charges is known as "unused material". The investigator is supposed to keep all material that appears to have some bearing on any offence under investigation or any person being investigated or on the surrounding circumstances unless it is incapable of having any impact on the case. The investigator is under a duty to alert the prosecutor to the existence of relevant material that has been retained in the investigation. This is known as "revelation". Revelation to the prosecutor does not mean automatic disclosure to the defence.

"Revelation" consists of the investigator providing a schedule of the unused material to the prosecutor. There is scope to designate certain unused material as "sensitive", that is, material which the investigator believes that disclosure would give rise to a real risk of serious prejudice to an important public interest; reasons must be given. Chapter 8 of the CPS disclosure manual sets out these "public interests", which include protecting the security and intelligence agencies, the willingness of citizens, agencies, commercial institutions, communications service providers etc to give information to the authorities in circumstances where there may be some legitimate expectation of confidentiality, protection of witnesses against intimidation, national (but not individual or company) economic interests, the use of covert human intelligence sources, and the protection of secret methods of detecting and fighting crime.

But it is for the prosecutor to determine, not the investigator. The CPS Disclosure Manual says: "The prosecutor must be satisfied that the risk is real, not fanciful. The prosecutor must be in a position to explain to the court the ground upon which it is asserted that there is a real risk of serious prejudice to an important public interest." Where the prosecutor decides that sensitive material requires disclosure to the accused because it satisfies the disclosure test (might reasonably be considered capable of undermining the case for the prosecution against the accused, or of assisting the case for the accused) and, in consultation with the police, that it is not possible to disclose in a way that does not compromise the public interest in question, and that disclosure

should be withheld on public interest grounds, the ruling of the court must be sought or the case abandoned. Courts can issue a Public Interest Immunity (PII) order limiting disclosure if they are persuaded by a prosecutor's arguments.

Thus the law enforcement officer contemplating the deployment of hacking techniques and concerned that undue publicity of the detail might prejudice future investigations as well as opening opportunities for the defence in the current case to argue that evidence has been contaminated, is at the mercy, in the first instance of the prosecutor and then the judge.

---

[i] http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/1827
[ii] http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf
[iii] Principle 3
[iv] http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/code-practice-electronic-info?view=Binary
[v] NAT: Network Address Tranlation
[vi] The position of SIS (MI6) and GCHQ is addressed in the Intelligence Services Act 1994, ss5 & 6.
[vii] http://www.cps.gov.uk/legal/d_to_g/disclosure_manual/disclosure_manual_chapter_27
[viii] The technical name is WLAN (Wireless Local Area Network) and the standard used is in the IEEE802.11 family
[ix] WEP or WPS
[x] http://en.wikipedia.org/wiki/Evil_twin_%28wireless_networks%29
[xi] s 28 RIPA, 2000
[xii] http://hassam.hubpages.com/hub/Types-Of-Bluetooth-Hacks-And-Its-Security-Issues; http://techpp.com/2010/06/30/7-most-popular-bluetooth-hacking-software-to-hack-your-mobile-phone/ http://trifinite.org/Downloads/trifinite.presentation_blackhat.pdf
[xiii] Criminal Procedure and Investigation Acts, 1996 and 2003
[xiv] http://www.cps.gov.uk/legal/d_to_g/disclosure_manual/.