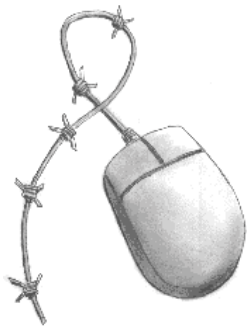
GreenNet CSIR Toolkit Briefing

Privacy and Surveillance



How and when organisations and the state can monitor your actions

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

The art of surveillance has been practised throughout history. Sun Tzu's *The Art of War*, for example, written in the Fifth Century BC, contains a chapter on *The Use of Spies*[1] where he describes the different ways spies may be used to monitor enemy forces.

The most crucial development that has taken place, with the rise of democratic states, over the last two to three hundred years, is that the focus of state surveillance has shifted from external threats to the monitoring of the state's own population.

Nowadays, despite national and International agreements that give individuals rights to privacy and a fair judicial process, the practice of surveillance is growing in complexity, thanks to the spread of electronic networks. It is increasingly being used by the private sector for economic purposes, and by the state for security purposes.

State surveillance exists to counter a variety of perceived threats, from subversion by other states to external or internal terrorism and the activities of organised crime. Much of this surveillance has, historically, been carried out by human operatives, and hence was limited in its scope. But surveillance today is increasingly automated, with high speed computers facilitating many of our everyday activities (from mobile phone calls and email to credit card transactions).

This process of automation opens up new opportunities for mass surveillance of the Internet and telephone networks, as well the development of data profiling of individuals. Mass surveillance is increasingly being initiated by the private sector as a means of protecting intellectual property rights.

Whereas one of the central issues of debate in the twentieth century was the democratic process within the state, in this century it is likely that major concerns will be around the privacy of the individual within the new 'information society'.

This briefing outlines the range of surveillance techniques in common use today. It also looks at potential threats to civil liberties posed by the use of electronic networks for the purposes of surveillance, by the state and private companies, and the potential damage of these for civil society in the long term.

[1]Chapter XIII, *The Art of War*, by Sun Tzu. This can be found at many locations on the Internet if you conduct a search for the title and the author's name.

Passive surveillance - *dataveillance and data profiling*

The Hollywood-style cliché of surveillance activity is of state security agents listening to radios, or using hi-tech gadgetry to monitor the activities of a single individual[2]. This actually applies to only a very few people within society whom states actively target - crime bosses, for example, or international terrorists.

Nowadays computers and databases of information are widely and very effectively used to monitor networks of people - the term 'network' applying to anything from a political organisation to regular shoppers at a large supermarket. This practice is often known as *dataveillance*.

Data profiling

Modern services are increasingly operated using networks of computers. The technology employed by these systems often creates a *unique identity* for you when you use them. Your telephone number, your bank account number and even your car number plates are examples of these unique identifiers. When you use the Internet to browse a web site, or send an email, your email address, or your computer's Internet Protocol (IP) address are your unique identifiers.

These unique identifiers can be used to track certain of your actions by computer; they help to create a *key* through which to extract information about you from a database. By combining a number of these databases, using many different search keys, it is possible to produce a profile of your activities that (depending on the kind of databases used, and the means by which information is matched and abstracted) gives a fairly accurate, if limited, description of your activities (such as your telephone or Internet use). This process is called *data profiling*[3].

Techniques like data profiling are sometimes known as *passive* surveillance because they do not monitor an individual directly; rather, they monitor the *paper* or *audit trails* that you leave behind as you go about your everyday life.

Dataveillance and data profiling are often used as (fairly innocuous) market research tools, to analyse food sales for a supermarket chain, for example. In these cases the focus of the data analysis is not so much on your personal identity, but on particular patterns of activity (i.e. what people buy at the supermarket), enabled by the various keys in the database. You yourself will be unaware that this data profiling has taken place.

Increasingly, however, individual identity is central to the whole reason for processing data. Dataveillance is being used, for example, for:

- *Direct marketing* - where individuals are targeted for some form of advertising or lobbying based on their known buying habits;
- *Political lobbying* - where political parties increasingly use dataveillance as a means of identifying floating or swing voters in key marginal constituencies, in the hope of targeting election campaign resources more effectively;
- *Police investigations* - where databases which log activities such as credit card transactions and mobile phone calls are used to target individuals as part of serious crime investigations. Police are increasingly using DNA samples as a means of identifying people, and retaining them on

[2] A good description of this model of surveillance is available in Peter Wright's book, *Spycatcher*, which the British Government tried to ban during the mid-1980s. As one of the technicians responsible for surveillance, he described in detail the means by which people can be directly monitored.

[3] For a more detailed account of the use of data as part of dataveillance and data profiling, see the book *Big Brother* by Simon Davies (Pan Books, 1996).

database for future reference;

- *Protecting intellectual property* - where many new intellectual property rights protection systems[4] rely on information being embedded in computer programmes or data processing services; this information uniquely identifies you as the purchaser or licensed user, and makes it possible to track and monitor your use of that software or service.

Use of dataveillance is currently limited by the variety of database keys that exist. Its effectiveness could be increased, from the perspective of those making use of it, by some form of standard machine identification that would function as a master key to all other databases. Proposals for machine-readable identity cards, or some form of standardised online authentication (such as a unique *digital signature*, favoured by some states as part of *key escrow* or *trusted third party* systems[5] to verify identity in data encryption)[6] threaten to do just this. Such cards or signatures would act as a 'master key' for other systems to authenticate access or transactions.

One of the main objects of developing paper or audit trails for dataveillance is to prove identity. However, there are already systems that can provide authentication for a transaction without requiring absolute proof of identity. Mathematical algorithms can by used by IT systems to prove that you are presenting the correct authentication to enable the transaction (such as debiting a bank account, for example), without the need for the system to divulge your identification, you bank account details, or other identifying keys when you make that transaction. Systems like this would limit dataveillance potential to those sorts of information to which a person consents.

The new generation of authentication systems have not yet been widely adopted. The banking corporations responsible for maintaining the systems prefer mechanisms that require some form of personal identification. Because of their interests in tracking people's activities, states and security services may also resist any change to the current system that makes identification a condition for authenticating transactions.

Online surveillance

The Internet operates on a world-wide basis. It is increasingly being used not only as a means of dataveillance, but also for more active surveillance of individuals or groups. Your unique identity on the Internet provides an excellent master key by which to monitor your activity on the Web.

When you access the Internet through a network or via a dial-up account, your IP address is not usually fixed. It is therefore not possible to identify you personally as the owner of data packets that move across the Internet. Depending on the design of your system, however, or if you have been allotted a fixed IP address, it may be possible for packets of data to be directly traced to you. This means that your interaction with other Internet sites can be directly monitored by the state (see the section on *Directed surveillance* below).

Your email address, on the other hand, *is* unique and can be traced directly. However, although it is possible to show that a particular email address has been used, it is not possible to prove that the person to whom that address belongs was responsible for using the address at that particular time. It is also possible to forge or 'spoof' email addresses, making absolute proof more difficult. However, as more people use *digital signatures* to prove the authenticity of their email addresses, and because these signatures require passwords to enable their use, they can provide additional corroboration of the source of an email.

[4] See the GreenNet CSIR Toolkit Briefing no. 7, *Intellectual Property*
[5] See the GreenNet CSIR Toolkit Briefing no. 3, *Using Encryption and Digital Signatures*
[6] In the UK, the system for registering bodies responsible to holding electronic signatures as official 'third parties' was established in the *Electronic Communications Act 2000* - http://www.legislation.hmso.gov.uk/acts/acts2000/20000007.htm

The Internet, the World Wide Web and the services associated with it are being used more and more as a means of monitoring people's online preferences.

One of the better known ways of doing this is through *cookies.*[7] These are small files installed on your computer by the web server with which you are transacting data. Cookies store information about the preferences you choose within a specific website, and enable the site to personalise the services it offers you. They also provide an effective means of monitoring your use of the site. Some sites trade this information on to others for different purposes. A good example of this was the controversy involving the Internet advertising agency *Doubleclick*, and their use of information gained from web cookies.

Risks to privacy

Increasingly, the use of proprietary tools or services on the Internet comes at some cost to privacy.

For some time now it has been possible to embed, or encode, within the content of a computer file information on the person, computer or software programme that created the file. This means that anyone with access to digital versions could identify not only the author but also the registration details of the software tool used.

This now applies to the Internet. Web browsers, and some of the proprietary plug-ins that browsers use, pass information about their users back to home base. Companies do this in an attempt to protect their intellectual property.[8]

The privacy implications of the use of these tools are increasingly problematic; a growing number of software tools can only be registered online, which usually entails the transfer of information (about you as the user and about your computer) over which you have no control. Microsoft's *XP* operating system is a recent example of this.

Internet firewalls[9] are another illustration of potential for the invasion of privacy. Some of these programs, such as Real Networks' *RealPlayer*, try to connect to the Internet to transfer information even when you are not using them. Regular communication between programs installed on your computer, and their home source, is likely to become more common. It is also likely that, as restrictions on the use of certain proprietary information grow, these programs will also transact data about your usage of the program, not just the fact that it is installed on your system.

The other aspect of accessing information via the Internet is that a large number of *log files* are generated on your computer, on your service provider's computer, and on any computers you have been connected to. This data is not directly readable - for the most part it consists of *traffic data* that identifies the source of requests, the names of files that were supplied, dates, times, etc. But it can be of use to anyone monitoring the activities of groups or individuals, because it enables them to generate a profile of what people have been doing together online, what other systems or email addresses they have contacted, and the times, dates and even locations of communications between members of a network.

The use of such traffic data is becoming more and more controversial. If you work online you should be

[7] For information on the privacy implications of cookies see the Electronic Frontier Foundation's 'profiling, cookies and web bugs' page, http://www.eff.org/pub/Privacy/Profiling_cookies_webbugs

[8] See the GreenNet CSIR Toolkit Briefing no. 7, *Intellectual Property*.

[9] Internet firewalls police the programs that can be connected to the Internet when you are online. You have to personally authorise each program to connect to the Internet. Any programs that are quietly trying to connect to the Internet in the background, without your intervention, will be blocked, and you will receive a warning message.

aware that your activities, even if erased from your own system, can probably be tracked by assembling log files on other systems on the Internet (see the section on *Traffic data* below).

Directed surveillance

So far we have only considered the *indirect* monitoring of people, through their computers or on the basis of analysing data. *Directed surveillance* targets and monitors specific individuals directly. It falls into three main categories:

- Tapping communications;
- Bugging places of work;
- Using human operatives to monitor or infiltrate the target's activities.

In the UK the use of directed surveillance was updated and extended by the *Regulation of Investigatory Powers Act 2000,*[10] and the *Terrorism Act 2000.*[11] They update the powers of the state to tap communications and to infiltrate networks or organisations. These laws require that any directed surveillance must be properly authorised by a person empowered to do so, that this authorisation must be subjected to scrutiny to ensure that it was justified under the relevant law, and that that it was correctly applied.

For the most part directed surveillance can only be used where there is clear evidence that some form of serious crime is being, or is about to be, committed. Directed surveillance uses more resources than indirect monitoring, and this in turn restricts the number of people that can be watched at any time.

Following the attack on the World Trade Centre in September 2001, the UK Government decided that the Terrorism Act 2000 was not sufficient to deal with the threat of terrorism. It was therefore updated by the *Anti-Terrorism, Crime and Security Act 2001*[12]. This strengthened the powers of the state to hold traffic data. It also allowed government department to pool their information on terrorism and serious crime as part of investigations.

Surveillance of mass protests

For some kinds of directed surveillance controls are not so clearly delineated. These are enabled primarily through other general powers given to the police to 'maintain order'.

The policing of demonstrations in the UK over the past ten years provides an insight into the potential for using a variety of computer-related media to monitor the activities of many hundreds of people, and the potential for this process to be used in a manner that impacts upon civil liberties. As this type of surveillance does not necessarily directly target specific individuals, it occupies a grey area in terms of regulation.

The surveillance of demonstrations is carried out as part of a blanket authorisation from a senior police officer. The *Security Services Act 1996*[13] and the *Police Act 1997*[14] contain clauses which state that concerted action by many people, even if in itself it is not illegal, may be investigated as 'serious crime'.

[10] *Regulation of Investigatory Powers Act 2000* - http://www.legislation.hmso.gov.uk/acts/acts2000/20000023.htm
See also the GreenNet CSIR Toolkit Briefing No.13 on *Interception Capabilities*.
[11] *Terrorism Act 2000* - http://www.legislation.hmso.gov.uk/acts/acts2000/20000011.htm
[12] *Anti-Terrorism, Crime and Security Act 2001* - http://www.legislation.hmso.gov.uk/acts/acts2001/20010024.htm
[13] Section 2, *Security Services Act 1996* - http://www.legislation.hmso.gov.uk/acts/acts1996/1996035.htm
[14] Section 93, *Police Act 1997* - http://www.legislation.hmso.gov.uk/acts/acts1997/1997050.htm

Over the past ten years a special police unit has attended many demonstrations where people have expressed dissent from government policy. This unit records the demonstrators via video and still cameras. The police have also built up records on people's identities by taking photographs and fingerprints of demonstrators held in custody.

With many demonstrations and protest actions now being co-ordinated via the Internet, data profiling material is increasingly being combined with information obtained through directed surveillance. This information is probably filed and combined with that obtained by the police from other databases, to provide a profile of the people involved in demonstrations. There is no clear breach of the law here, but the data is being collected on the grounds that it *may* be useful for future reference, and not for specified purposes.

Network surveillance and the value of traffic data

Directed surveillance must be authorised on the basis of some evidence of wrongdoing by the target person or group. Section 12 of the *Regulation of Investigatory Powers* (RIP) *Act* widened the scope of powers for surveillance and introduced a new requirement for telecommunications service providers to install special taps to facilitate blanket surveillance based around the automated collection of traffic data.

This is not the same as directed surveillance, however. The Act draws a distinction in this regard between the *content* of a communication, and the *communications data* that is attached to the communication.

Communications data is information which describes the form of the communication, where it came from, and where it went, where it was routed along the way, how much data was carried, and how long it took to transmit.

The problem is that communications data, although it does not contain a message, when recorded and profiled in combination with that of other databases, can provide an extremely accurate picture of an individual's life, political or social activities and the network of contacts or friends with whom they carry out these activities.

This capacity can only increase, as new communications protocols provide far more information about geographical locations, and about the technology being used to create the communication, as part of the pool of data.

Section 5(3) of the *Regulation of Investigatory Powers Act* required that message contents should only be read in cases involving:

- national security;
- the prevention of serious crime; or
- the protection of the 'economic well-being' of the UK.

Section 22(2) of the Act, however, provides that communications data may be intercepted for the three purposes noted above, and also:

- in the interests of public safety;
- for the protection of public health;
- the collection of tax or charges payable to a government department; or
- for preventing death or injury.

Controls over communications data are therefore less restrictive than those for directed surveillance. Communications data is accessible to local government agencies as well as the police or security services.

The new *Cybercrime Convention*[15] also permits communications data to be routinely databased and held for many years, and shared with other states that are signatories to the Convention.[16] We could therefore face a situation, a few years hence, whereby communications data is not only accessed by our own government offices, but also for purposes devised by other states' security services.

The tapping of data communications is not the only way by which the state can obtain data on your electronic activities. Many modern networks, such as bank cash machines, mobile phone systems, wireless computer networks, and nearly all credit card payment systems, also archive information on where you were when a particular transaction was made. This facility for geographical tracking also provides opportunities for monitoring how people work together. Meetings between a group of people could be assumed to have taken place, for instance, if their mobile phones were all found to be in the same communications cell on the same day at the same time, or if they used credit cards or cash machines in the same area.

Once it is databased and archived (for four to seven years), communications data can be used, at very little cost or effort, to produce data profiles on thousands or tens of thousands of people. It is for this reason that the collection of communications data represents a threat to civil liberties. It means that in any investigation into a person's activities, a large pool of data could be immediately available. This could give rise to situations where investigators attempt to fit the person's data profile to a crime. This has already been alleged as happening in a number of miscarriage of justice cases where a person has been convicted solely on the basis of forensic or circumstantial evidence, without witnesses to corroborate the evidence.

As was seen in the recent legal action against the Metropolitan Police by the McLibel Two[17], there are instances where the authorities may release information covertly to non-governmental agencies - in this case, the former policemen who made up the McDonalds Corporation's corporate security team. But there have also been instances, such as the Bignell case[18], where information held by security or police authorities has been accessed for private, and perhaps even criminal, uses.

The significance of communications data to privacy and human rights are now being actively debated in the USA. This is because of various measure brought in as part of general measures to improve 'homeland security'[19]. In the UK, although the law has enabled the same mass surveillance, practicality is delaying matters. Currently there is no agreement between government and Internet operators on how they will enact these new laws. The proposals would require that service providers archived very large quantities of data, and this has a significant operational and economic impact on their business.

Privacy - *the public issue of the 21st century?*

It has been reported that up to seven per cent of the former state of East Germany's Gross Domestic

[15] *Council of Europe Cybercrime Convention* - http://conventions.coe.int/treaty/en/projects/FinalCybercrime.htm

[16] See also GreenNet CSIR Toolkit Briefing no. 8 on *Cybercrime*.

[17] After McDonalds security team members revealed that the Metropolitan police had passed intelligence information to McDonalds staff, the McLibel Two brought a suit against the Metropolitan Police for 'malfeasance in public office'. This was settled out of court earlier this years, following a payment to the Two, and a public apology from the Police Commissioner.

[18] The *Director of Public Prosecutions* (DPP) *v. Bignell* case (1998) relates to a failed prosecution against police officers who obtained information from the Police National Computer (PNC) for personal use. Other investigations have revealed that criminal gangs have on occasions been able to access information from the PNC using the services of police officers willing to accept money for providing information.

[19] Washington is watching, BBC News Online Thursday 28th February, 2002 - http://news.bbc.co.uk/1/hi/world/americas/1845515.stm

Product (GDP) was tied up in some way with state surveillance - either directly through the *Stasi* secret police organisation, or through the processing of information gathered from a wide variety of sources in East German society. This system has the closest resemblance to George Orwell's *Big Brother* in his book *Nineteen Eighty-Four*. Disclosures since the fall of the East German government have shown, however, that a large proportion of the information gathered was either partially or totally incorrect.

The main problem with surveillance systems based upon communications data and dataveillance is that they rely on a system of rules, based on *terse logic*, which enable information to be processed automatically. Because of the complexity and volume of information involved, collection and processing of communications data is almost entirely computer-based. The lack of human intervention means that the validity of any abstracted information cannot be audited independently (without further directed surveillance; it is only possible to check the information against that in the database - and that may have been incorrect in the first place). As with the *Stasi* records system, there are significant pitfalls in using data collected for one object for a completely different purpose; parameters that did not exist in the original means of collection may be erroneously read into a piece of information when set in a different context.

As with direct marketing or the keeping of public records, many errors can occur within the process of data collection and collation. Experience therefore shows us that a system of intelligence based upon communications data is likely to produce many *false positives* (where people's private lives may be needlessly intruded upon due to errors in profiling, for example) as well as *false negatives* (where the activities of a terrorist group, for instance, are overlooked because the terse logic of profiling systems does not correctly identify them).

This is why the issue of privacy arises when we consider the impact of widely networked information about large numbers of people.

Data protection laws were first developed in the 1970s with the objective of preventing inaccurate information being held on computer databases. But as databases have grown in scale and complexity their potential uses have outstripped the ability of the public, or data protection agencies, to keep abreast of any breaches of the law.

It could be said that the use of innumerable databases, and the profiles of our everyday activities that can be created as a result, has produced a new threat to personal privacy - the threat of intrusion into a person's personal convictions or political beliefs.

The corporate sector

Beyond the activities of the state, the most direct and common intrusion into personal privacy is likely to be as the result of the corporate use of private information. As well as direct marketing, data profiling can be used for:

- corporate recruitment processes. An example of this from the 1970s was a system developed by the Economic League that attempted to eliminate those with strong trades union sympathies from being employed by any major British corporations[20];
- the purposes of insurance cover or claims. Information on personal purchases (types of food, for example, or cigarettes) could be used by insurance companies as part of setting premiums or deciding on whether to provide cover at all;
- workplace surveillance. Monitoring of work activities and profiling of individual employees can be

[20]For a more detailed review of 'pre-technological' corporate surveillance and blacklisting see *The Technology of Political Control* by Carol Ackroyd, Karen Margolis, Jonathan Rosenhead and Tim Shallice (First edition published by Penguin in 1977, and a revised Second Edition was published by Pluto Press in 1980)

used as a means of ensuring the highest possible productivity levels, irrespective of the stress or poor morale that this may cause. This is particularly the case in businesses such as call centres where information technology is intensively used;

- enforcing intellectual property rights to protect monopoly interests. Monitoring information from databases or computer networks can provide evidence with which to track down copyright infringement, for example. The data produced as applications send data back to base can provide a means of monitoring individual use of proprietary systems;
- identifying vehicles and tracking individuals' movements. Systems are able to link high-quality CCTV images to a computer database, in order to identify the presence of certain persons or car number plates;
- hi-tech crime. The accumulation of a sea of data will provide new opportunities for the misuse of personal data for fraudulent purposes, to mask other activities such as theft, and perhaps even the use of personal data for extortion or intimidation.

Current laws would allow all these operations to take place, within the restrictions provided under data protection law.

What price for privacy?

The only obstacle in UK law, other than data protection laws, to the use of personal data for any purpose is contained in the *Human Rights Act 1998.* Under the provisions of Article 8 of the *European Convention on Human Rights* state:

- Everyone has the right to respect for his private and family life, his home and his correspondence.
- There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Under UK law, therefore, a person has no *absolute* right to privacy, or for respect of their private life, correspondence home or family. As these rights are subject to Article 8 (2) above, there is clearly a wide range of circumstances in which government and other bodies could argue for exceptions to be made.

It remains to be seen how widely the definition of what constitutes a 'public authority' will be interpreted by the courts, but it is clear that some companies and non-governmental organisations can be deemed public authorities (very broadly speaking, because they offer services to the public).[21]

So in situations where data has been used, even if the information was erroneous, in a way that damages a person's private life, individuals have limited legal rights to prevent further disclosure or to seek redress for the damage caused (unless they could prove the material was libellous, which in practice is not easy).[22]

[21] The decision as to whether a particular company can be considered a public authority is dependent upon the levels of legal rights granted to it under public law - for example utility companies. This principle was established following an employment tribunal against British Gas during the 1980s. But the principle is still evolving as new cases a brought against companies with varied public functions - for example those who form part of recent 'private finance initiative' (PFI) projects.

[22] See the GreenNet CSIR Briefing no.9 on *Expression and Defamation.*

The growth of networked databases of information has come about as a result of the economic imperatives of corporations who seek to control and organise their activities, and through the willingness of the public to trade some of their privacy or anonymity for the benefits of cashless payments, or incentives to shop. But as the state and corporations find new uses for the data they hold, these benefits will seem a poor reward to some. For others, subject to exclusion or discrimination on the basis of data profiling, the collection and use of data could constitute a significant threat to their human rights.

Recent developments mean electronic transactions do not need to be authenticated with evidence of personal identity. These systems impact on personal liberties because many of them include information on identity.

Nevertheless, the new communications opportunities presented by new technologies need not necessarily endanger civil liberties. Information on identity can be separated from transactions, maintaining an appropriate level of anonymity and privacy.

Likewise, closer control over the uses to which personal information may be put (especially in relation to data profiling as part of determining a person's suitability for work, insurance cover, etc) are desirable, and there should be a process of review to ensure that any data profiles produced are accurate. Such possibilities exist at the present, under the *Data Protection Act 1998*[23]. But, for the moment, the time it takes for an individual to obtain and check the information held on them (in many different databases) makes it impossible to ensure that inaccurate information will not be used in decisions made about our lives.

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 surveillance, whether by the state, or by private organisations?
- Do data protection laws provide sufficient rights to track down and prevent inappropriate uses of personal information on databases, and does that include data held by the state?
- To what extent does the law provide exceptions for surveillance involving the use of communications data?
- How widely available is communications data to state or private organisations?
- Does your state intend to adopt the proposals on sharing communications and surveillance data contained in the *Cybercrime Treaty*?

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 on state or private surveillance.

The GreenNet Internet Rights Project

[23] *The Data Protection Act 1998* - http://www.legislation.hmso.gov.uk/acts/acts1998/19980029.htm See also the GreenNet CSIR Briefing on *Data Protection*.

GreenNet[24] is the UK member of the Association for Progressive Communications[25] (APC), and is leading the European section of the APC's Civil Society Internet Rights Project[26]. 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.

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[27] 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] GreenNet - http://www.gn.apc.org/
[25] APC - http://www.apc.org/
[26] CSIR Project - http://rights.apc.org/
[27] http://www.internetrights.org.uk/

