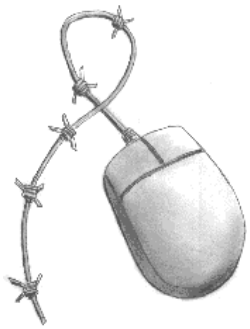
GreenNet CSIR Toolkit Briefing no. 10

Electronic Rights in the Workplace



Changes to workers rights and employers responsibilities in the new information economy

Written by Paul Mobbs for the
GreenNet *Civil Society Internet Rights Project*, 2002.
http://www.internetrights.org.uk/

The new information economy has led to a change in the employment practices of many companies. Whilst many people look on the jobs created by the information economy as "high tech", in many respects new levels of de-skilling and pay differentials have been seen.

Some parts of the new information economy, such as telesales or call centres, and some information processing jobs such as web content production, have been likened to the sweatshops of traditional manufacturing industries. Even better paid jobs have high job insecurity.[1]

This briefing provides an introduction to some aspects to working in the new information economy, and suggests sources of further information. It is intended to be of use to individuals and organisations working in the IT industry or in any workplace which uses information technology and new media.

Contracts

Information technology has a far higher proportion of temporary and short-term contract workers than many other industries. The IT industry has evolved the new job definition of *permatemp* - someone who is kept on a regularly reviewed short-term contract. The high speed of technological change in the industry means that specialisation does not always result in long-term employment. There is a continual pressure to upgrade or update your skills in order to keep your employment potential high.

More stable jobs, such as routine systems administration or web site production, do not carry the high rewards of other jobs in the sector, but can be equally insecure.

What determines the standards of any job is the employment contract. In the USA, the IT industry maintains its flexibility by keeping many IT jobs on low-specification contracts (and as a result there have been calls for a union for IT employees in the US).[2] In Europe it is not so easy for companies to do this, because of various employment rights granted as part of European Directives.

The approach of short-term or regularly reviewed contracts in the UK has recently been challenged because of reforms to the national insurance rules. Self-employed people pay their own national insurance

[1] For a well-written review of the employment trends in the new information economy see the book *Net Slaves - True Tales of Working the Web*, Bill Lessard and Steve Baldwin (McGraw-Hill, 2000)

[2] A good example of the work in relation to workers in the IT industry is the Communications Workers of America web site - http://www.cwa-union.org/

contributions, but on a lower rate than the equivalent total paid by an employee and employer's contributions. The new rules propose that freelance workers whose main income comes from one contract should be treated as employees. This has met with great opposition from within the IT industry; employers say it would increase costs and remove their flexibility by being able to dispense with staff at short notice.

The status of many freelance workers has been challenged by the new European *Working Time Directive Regulations,*[3] which set limits on conditions relating to hours of work and entitlements to time off. The regulations define employment status in relation to:

- Whether the individual is paid a regular wage or salary, or whether they invoice for work;
- Whether they or the employer deals with the payment of tax;
- Whether they are free to accept or decline further work;
- Whether they are free to do the same type of work for more than one employer;
- Whether they subcontract or employ their own staff;
- Whether the acceptance of work carries some form of financial risk as part of the contract;
- The level of responsibility they take for management within the company; and
- Whether, as part of their management role, they stand to profit through bonuses and other incentives.

Where no contract of employment exists, basic rights as provided in law apply. It is rare, however, for people in the IT industry to be employed without a contract because of the confidentiality or intellectual property implications of many jobs.

If you are classed as self-employed, you:

- Are liable for your own tax and national insurance payments - which necessitates registration with your local tax office as a self-employed person;
- Are not covered by ordinary employment protection laws, especially in relation to conditions of employment, maternity rights, sick pay, redundancy, dismissal and equal pay. Any dispute must be resolved as a breach of contract;
- Are not usually covered by the employer's compulsory workplace insurance for industrial injury;
- May be personally liable for any problems or damages that arise from your own work - which means that unless you set up as a limited company, you may be exposed to unlimited liability for any damages that are attributable to your work.

An employer can gain a number of operational and tax advantages from transferring someone from employed to self-employed status. An employee should think very carefully about changing their employment status, because of the potential loss of rights and liabilities involved.

An employer can require reasonable changes to working practices, but they cannot make a person change to being self-employed without some form of agreement, or by first making them redundant; otherwise, the person has a claim for unfair dismissal.

Privacy at work

The computers that people use, for example as part of work in call centres, or even at the highest levels of

[3] *Working Time Regulations 1998*, SI. 1988/1833 - http://www.legislation.hmso.gov.uk/si/si1998/19981833.htm

computer programming, can be made to monitor the work of individuals as they perform their duties. Sometimes the monitoring of employees' work is justified on the basis of security, especially where workers handle sensitive personal data or financial transactions.

Monitoring of employees at work, however, sometimes used as a means of assessing performance against imposed targets, and as such may be a form of intimidation. This is especially true of call centres, data processing and data entry workplaces, where speed of operation is crucial to operational performance.

The use of surveillance in the workplaces is rapidly increasing. A study published by the American Management Association[4] found the number of companies in the US conducting some form of 'active monitoring' of employees rose from forty-five per cent in 1998 to seventy-four per cent in 1999; e-mail monitoring rose from twenty-seven to thirty-eight per cent over the same period.

In the UK the law on workplace monitoring of communications was formalised in the *Regulation of Investigatory Powers* (RIP) *Act 2000.*[5] This provides that the owner of a private telecommunications system may monitor that system lawfully, within certain limits.[6]

The monitoring of the communications and activities of employees in the workplace in the UK must, however, be balanced with requirements under the *Human Rights Act 1998* and Article 8 of the *European Convention on Human Rights*; organisations must have regard to the private lives of individuals. Further guidance on surveillance in the workplace in the UK can be obtained from Institute of Employment Rights.[7]

Some workplaces, particularly within the larger (mainly US) corporations also employ workplace alcohol and drugs testing. This is often stipulated as a condition of the contract of employment. Such terms, following a trend that began in the USA, are seen as a way of ensuring the reliability of employees. Unless you have signed an agreement in a contract of employment, however, searches of your possessions or testing for alcohol, drugs or other materials cannot legally take place without your consent.

Even if you have signed an agreement on testing, if on some occasion you refuse testing, and such testing is attempted against your wishes, then that would constitute bodily assault and you would be entitled to resign and sue for constructive dismissal.

Use of the Internet in the workplace

The email and Internet services provided in the workplace are the property of the employer. If, as part of a contract of employment, or as part of any accessible workplace handbook, there is no explicit ban on personal use of these services, you can use them provided it does not detract from your duties.

There have been some instances where employers have used the use of the Internet as grounds for dismissal.[8] If you have not previously been told that these services are for work-related use only then you should receive no more than a verbal or written warning. You could only be dismissed if there was a clearly stated company policy that staff were routinely made aware of (for example, notices on every computer or

[4] See http://www.amanet.org/research/pdfs/monitr_surv.pdf for a copy of the report.
[5] See http://www.legislation.hmso.gov.uk/acts/acts2000/20000023.htm
[6] The guidelines, that apply to some private telecommunications systems, are formalised in *The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000* - http://www.legislation.hmso.gov.uk/si/si2000/20002699.htm
[7] *Surveillance and Privacy at Work* by Michael Ford is available from the Institute of Employment Rights, 177 Abbeville Road, London SW4 9RL.
[8] ZDNet UK News: *Net surfing could get you sacked* - http://news.zdnet.co.uk/story/0,,s2073980,00.html

on a notice board).

Attempts to break the security of user accounts or network security are only classed as "misuse of computers", and a breach of the *Computer Misuse Act 1990*, if the employee does not ordinarily have authorised access to the system. If there is a clearly stated policy on the limits of an employee's rights to access the system, an attempt to break security systems could be grounds for dismissal on the basis of gross misconduct. The *Computer Misuse Act* only covers "unauthorised" access to computer systems.[9] However, if an employee succeeds in accessing areas of the system which result in the disclosure of sensitive personal information they could be subject to prosecution under the *Data Protection Act*. If an employee used the workplace computer system to crack the security of another computer system that their employer did not control, then that would constitute a breach of the *Computer Misuse Act*.

In terms of the use of Internet services by employees there are various liabilities that staff and employers need to be aware of. Clear policy guidelines should be made as part of the condition of staff using the services provided by the employer:

- *Defamation* - material published on a company web site or sent via email could, in theory, be libellous. For this reason there should be specific disclaimers within email signatures, and on any other services such as web sites, to provide a clear distinction between the employee's own personal comments and their statements on behalf of the employer. However, although the employer could claim, provided such disclaimers were in place, that they were not responsible for any defamation (under the defence of 'innocent dissemination' under section 1 of the Defamation Act 199610) they would have to remove any material alleged to be defamatory, and pursue appropriate disciplinary action against the employee, or they themselves would be liable for perpetuating the defamation.
- *Copyright infringement* - material published or circulated by employees, such as documents, software or music or multimedia files, could breach copyright. Copyright classes infringements as either primary or secondary.11 Provided that the employee had breached copyright in the course of their own private activities, it is unlikely that the employer could be held responsible for a primary breach of copyright. However, they could be liable for a secondary infringement of copyright law, in which case they would be required to take reasonable steps to identify and remove this material.

Employers should regularly review the information on their systems to eliminate copyright material they are not permitted to store. However, those areas of the system or off-line storage media (such as floppy disks) reserved for employees' private use are covered by the *Human Rights Act 1998* and Article 8 of the *European Convention on Human Rights*. The review of any private material held by an employee therefore requires the employee's permission, so companies must develop an agreed policy for the review of copyright on any materials employees hold privately within the workplace.

- *Confidentiality* - information made publicly available or e-mailed by employees may be confidential, and may represent a breach of trust if disclosed. There is no simple way for employers to deal with this, other than to provide clear guidance on how material is to be handled, and to ensure that the hierarchy of file storage and access permissions minimise the risk of accidental disclosure. Where an employer has an obligation to protect personal information, for example within organisations registered under the Data Protection Act, employees should be made aware of the data protection principles, and there should ideally be a statement within email signatures alerting recipients of information to the need to protect or destroy the email after receipt.
- *Sexual or racial harassment* - information circulated by employees that is sexually or racially offensive. Employers are liable under the Sex Discrimination Act 1975 and the Race Relations Act 1976 if they do not take reasonable steps to prevent abusive material being circulated from their

[9]See the GreenNet CSIR Briefing no.8 on *Computer Crime*
[10]See the GreenNet CSIR Briefing no.9 on *Expression and Defamation*
[11]See the GreenNet CSIR Briefing no.7 on *Intellectual Property*

systems (note, there is currently no clear sanction against homophobic abuse, unless it threatens specific violence against a named person). Employers are required to show they have taken all 'reasonable steps' to prevent their systems being used for spreading abusive material; a condition of employees' use of Internet services should include policies prohibiting the circulation of abusive material. Failure to apply these standards would then result in disciplinary action.

Intellectual property rights

The basis of the information economy is the defence of intellectual property rights, usually by commercial interests. Employees have an obligation to protect the employer's intellectual property rights. This may be dealt with as part of the job description, or by confidentiality clauses within a contract for consultants and self-employed workers.

Employees also have rights to protect their own intellectual property.

Many large companies today require, as part of a contract of employment, that they have the rights (or sometimes "first refusal" of rights) to anything that the employee creates during their term of employment. That does not just mean things created within the workplace, but may include anything the employee creates at home that is related to the function for which they are employed. There is no clear legal basis for this, and it could be challenged under human rights legislation. As yet there have been no legal cases which clarify this area.

Problems can arise are where:

- Employees use the employer's equipment and software in the home - the employer could claim that developments or information was produced at their expense; and
- Employees replicate parts of the information they use in the workplace at home - in which case the employer could argue that the employer has some rights to the material, or, if not, that the employee has breached the employer's copyright.

To avoid confusion, if an employee wishes to produce material in their own right then they should:

- Seek to obtain either a contractual demarcation of their own work from that of their regular employment (if it is produced within the employee's home); or
- If the employee intends to use the facilities provided by the employer, negotiate some official form of licensing agreement that reserves the employee's rights, or some form of leasing agreement that allows the employee to use the employer's facilities without giving over any rights to the employer.

Future changes in employment rights

Future changes in employment rights are likely to be closely linked to changes in technology, and especially to changes in controls over intellectual property rights. If computers become increasingly networked, for example through proposals such as Microsoft's "dot-Net" system, and with continued growth of *teleworking*, the divisions between employees' and freelance workers' conditions could become increasingly blurred.

There are two particular areas of change in the short term:

- The EU Social Chapter - As the UK adopts more elements of the Social Chapter, at some point differentials in improved job security and improved social benefits for permanent employees will have to be reflected in conditions for self-employed people. It is not yet clear if this will be required as part of contracts, effected through legislation on contract terms, or whether, much like the current arrangements in relation to the Working Time Regulations, it will be for the freelance and the employer to reach a mutual voluntary agreement.
- Teleworking - The potential of teleworking has so far been limited by the lack of infrastructure, and in particular the lack of broadband access. Homeworking used to be a key part of the manufacturing industry's outsourcing of work; broadband would allow similar changes to the IT industry. Rather than having data entry or call centre workstations in a central location, For example, they could be located in a person's home.

As noted earlier, problems arise in relation to the use of business equipment for personal uses, especially in relation to intellectual property rights and privacy. But more significantly, issues of health and safety and employment rights arise when people's main place of work is their own home, rather than their employer's main establishment. As laws on communications are progressively updated, to take account of new publishing and communications aspects of the Internet, there will have to be some renegotiating of existing employment terms to take account of teleworking.

Changes in communications technology over the next few years are likely to apply further pressure to European-based employers and encourage them to outsource IT work to other countries. This is already happening in the USA, where data processing bureaux have sought to develop twenty-four-hour processing of data by setting up 'outstations' in Asia.

So although the increasing use of technology may improve the options for people working within the IT industry in the UK, the ability of companies to move work and capital, under new free trade rules, to other states across the globe may create pressures that further restrict opportunities for employment within the UK IT and other sectors.

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:

- Do existing employment protection policies provide specific guidance on the use of resources at work, such as the Internet?
- Does existing employment law, perhaps as part of human rights law, protect the privacy of the individual at work?
- How do telecommunications laws define the legal position of monitoring employees in the workplace, and do they guarantee minimum standards of protection from dismissal and of privacy?
- To what extent does intellectual property rights law impose restrictions on employees in terms of their everyday work?

You should also contact any civil liberties organisations or trades unions (particularly those unions representing the IT sector) operating in your country. They may be able to provide you with much of the information you need on employment rights.

The GreenNet Internet Rights Project

GreenNet[12] is the UK member of the Association for Progressive Communications[13] (APC), and is leading the European section of the APC's Civil Society Internet Rights Project.[14] 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[15] 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.

Free Documentation License:

For more information about the Civil Society Internet Rights Project, or if you have questions about the briefings, contact ir@gn.apc.org.

[12] GreenNet - http://www.gn.apc.org/
[13] APC - http://www.apc.org/
[14] CSIR Project - http://rights.apc.org/
[15] http://www.internetrights.org.uk/