

# 'Big brother' web policies are legal

BUSINESSES worldwide are said to be losing more than £130 million every day to employees' excessive internet usage. That's almost £50 billion each year - so services such as Facebook, eBay and more "personal" offerings have a lot of blame to shoulder. Employers need to get to grips with this colossal waste of company time and, for once, the law doesn't need to get in the way.

Legislation such as the Data Protection Act and the Human Rights Act - and the many codes of conduct and guidance notes - are meant to offer certain basic protections. These include the right to privacy, the right to confidentiality, the right to participate in (online) society, and more esoteric ideas such as only keeping personal information that is accurate and necessary.

Employee monitoring, and restricting access to e-mail and the internet, seems therefore to be completely offside at first glance. As a result, businesses are often too conservative about using "big brother". Yet it can be OK to use closed-circuit television (CCTV), examine e-mails and record phone calls - or even restrict internet usage.

If you're in jail or in the army or somewhere else that makes it hard to make your own choices, you may have a good argument that CCTV or limited internet access is actually wrong. After all, you can't opt out of being filmed in the jail unless you have some useful ironmongery in your home baking. Similarly, a five-to-ten stretch in the forces' jail for refusing to allow your e-mail to be monitored is not an option that many will take.

For these reasons the courts are quite happy to intervene if these freedoms are infringed ... and there is no real consent that can be obtained from those affected.

Employees in the "free" world do, however, have a choice. If they don't like the rules they can leave - or they can refuse to join. As a result, the judges are much more reluctant to interfere, as long as it's open and upfront.

So, as long as a contract of employment says an employer can intercept e-mails or record phone calls or deny private

---

ALAN D STALKER

---

internet use, the law shouldn't be too much of an issue.

Even so, employers should remain, at least, a little cautious: keep an eye on what's reasonable in the particular circumstances, and make sure the rules are in place so that employees know what they are consenting to.

Most, if not all, monitoring with consent will be reasonable. If consent is impractical or pointless, reasonableness is more of an issue. The most common example relates to hidden cameras to monitor stock theft or the like. This can only be justified where there are grounds for suspecting criminal activity or equivalent malpractice and then must be really limited in scope and effect. Even small-print consent (in the employee handbook, for example) would still need to be considered in the light of what is reasonable.

The more difficult thing is to get the rules in place in advance. If you're going to forbid e-mail usage at work or intercept e-mail or whatever that interferes with the usual

**Employers shouldn't feel too afraid to make people do what they are paid for**

freedoms of civic society - and more importantly may want to take disciplinary action on the back of that ban - then you must make this clear in your contract.

Not only do you have to write it down, you may have to impose those rules on existing employees. There's not enough room here to dwell on that particular minefield but it can be done. It just has to be done carefully.

Employers shouldn't then feel too afraid to make people do what they are paid for (and forbid internet usage and personal e-mail if that gets in the way), and should be prepared to check that this is being adhered to (by monitoring what's happening, even if somewhat covertly).

What is essential is that employees agree to this upfront and are under no illusion of what can be monitored. Big brother can sometimes be a good thing!

● Alan D Stalker is a member of CCW Business Lawyers.