

Intercepting Communications

With more and more of our communications being sent electronically, over the internet and by email, fax and telephone, the security of such communications is of major concern. If you are sending sensitive or copyright information over such communications, protection of the communication is the first line in your defence of the information itself.

WHEN CAN COMMUNICATIONS BE INTERCEPTED?

Under the Regulation of Investigatory Powers Act 2000, it is a criminal offence for someone to intentionally intercept any communication that is sent by post or over a public or private telecommunications system.

Interception of communications is permitted only in a few strictly limited circumstances:

- the police and the security services have power to intercept communications where they have a warrant to do so.
- interception is permitted where both the sender and recipient have consented to it (this is the exception that is being used when you ring up your bank and are told that “some calls may be monitored and recorded for quality and security purposes” – by continuing with the call, you are implicitly consenting to such recording)
- interception is permitted where it is connected with the operation of the communications service itself
- the right of employers to monitor their employees.

MONITORING EMPLOYEES

The right to employers to monitor their employees is governed by the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, and is the exception that applies to most businesses.

For an employer to monitor an employee without their consent, they must comply with all the requirements of the Regulations. The monitoring must only be of business-related communications. Emails marked “Personal” should not be intercepted, unless the employer has reason to believe that the email is in fact business related.

The interception must ONLY be for an “authorised business purpose”. “Authorised business purposes” are:

- to establish the existence of facts
- to check that the business is complying with regulatory or self-regulatory requirements
- to check standards of employees or show the standards that employees should be achieving
- to prevent or detect crime
- to investigate or detect unauthorised use of the telecommunications system
- to ensure the security of the system and its effective operation.

In addition to ensuring that you comply with any requirements under RIPA, any information that is gathered must comply with the Data Protection Act 1998. For more information, please see our Factsheet on Data Protection.

FURTHER INFORMATION

The Information Commissioner has produced a Code of Practice for the monitoring of employees, which is available from www.informationcommissioner.gov.uk

For more information on monitoring employees, please see our Employment Factsheet “Monitoring Employees”.

MEDIA & TECHNOLOGY UNIT



Mark O'Halloran

office: 01293 643430

mobile: 07810 504556

email: mark.ohalloran@stevensdrake.com

