

Guidance to Recording Business Calls

It is widely (and incorrectly!) believed that it is unlawful in the UK in all circumstances to monitor and record telephone calls without drawing this to the attention of the parties to the call. There are in fact broad exceptions which are relevant to many businesses which do allow such activities without obtaining consent.

There are several reasons why businesses may wish to monitor or record telephone use for the purpose of its business. Often the rationale is quality control or even compliance by an employee with certain regulations, but the monitoring may also be useful for ensuring that employees are not calling friends in Australia at the businesses expense or otherwise using the system contrary to your policies. The law must however balance these goals against the need to protect employees as well as external persons from "snooping" and misuse of such data.

There are two principle legal areas of relevance; namely, the law on "interception" of communications stemming from the Regulation of Investigatory Powers Act 2000 ("**RIPA**") and the Data Protection Act 1998 ("**DPA**").

Regulation of Investigatory Powers Act 2000

RIPA puts constraints on when a person may make an "interception of a communication in the course of transmission". RIPA is wide in scope and, in particular, "interception" includes a "monitoring or interference" with a private telecommunications system which makes the communication available to someone other than the sender or recipient of the communication. Interestingly, this includes the opening of previously unopened emails, but for the purpose of this article, it includes listening in on and recording telephone calls.

Any interception would be, broadly, unlawful (in fact, criminal) unless the consent of both the sender and recipient is obtained, or alternatively the communication falls within an exception defined in the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (the "**Regulations**"). Under the Regulations, the exceptions that are relevant to most businesses are where monitoring or recording communications are carried out: to ascertain compliance with regulatory requirements, practices or procedures;

- to ascertain or demonstrate employee standards;
- for the purpose of preventing or detecting crime;
- for the purpose of detecting unauthorised use of the telecommunications system; or
- to ensure the effective operation of the system.

In addition, monitoring (but not recording) communications may be carried out without consent:

- for the purpose of determining whether they are communications relevant to the business; or
- to monitor communications to confidential anonymous counseling or support helplines.

In addition, in all cases where consent is not obtained, the interception must be of a communication *relevant to the business*.

This is all pretty wide, but there are two easy traps to fall into.

First, a business must not intercept private communications. Having said that what happens if what you thought was a business communication turns out to be private? It is easy to envisage a personal communication being inadvertently intercepted in the course of a permitted interception. Where this is the case there is no offence where the situation is unavoidable in the context of permitted monitoring. In other words, if in the course of the monitoring (or the playing back of a recording) it becomes apparent that the monitored communication is in fact private, the interception (or playing back) should cease.

Consistent with the situation under the data protection regime, below, an employer must have made all reasonable efforts to inform all employees that an interception of their telecommunications may take place.

Data Protection Act 1998

The recording of phone calls will also be governed by the DPA, as the information recorded will be "personal data" of an employee and (possibly) "personal data" of the external person (as the recording could be used to identify the caller). (Interestingly, merely listening in on calls does not raise a DPA issue, but making notes of what is discussed might.)

As such, the data protection principles set out in Schedule 1 of the DPA must be adhered to. In particular, all processing of personal data must be "fair". The one difficult issue here (which is why you often hear notices in relation to recorded calls) is that to be "fair" the following information must be provided to the individual, "so far as is practicable":

information regarding the identity of the "data controller" (broadly, the party 'processing' the data) and the purpose for which the information is being processed.

further information as is necessary, having regard to the specific circumstances in which data is processed, to enable the processing to be "fair".

Both the requirement that information only be provided "so far as is practicable" and the vague requirement to provide information which is "necessary" to be "fair" require an exercise of judgment and explains why some people do provide notices of recordings of calls.

Employees

The analysis above applies to employees as well as external persons, but for data applicable to employees in particular, the Information Commissioner has published a detailed Employment Practices Data Protection Code ("**Code**") which covers, amongst other things recording and monitoring of employee calls. Although the Code is not strictly binding, the Information Commissioner has been clear that enforcement of the Code will be based on breach of the DPA itself.

The Code sets out the core principles for monitoring of employee calls. Three key principles are:

Proportionality - an employer should be clear as to why the monitoring and recording is required and should determine whether the reason for it is legitimate. Against this reasoning, the employer should consider whether the action is as un-intrusive as possible. Employers should conduct an assessment of the impact of its monitoring in order to ensure the balance is appropriate.

The Provision of Information to Employees - in order to comply with the first data protection principle, full information about the monitoring or testing should be supplied to the employee. The Code is clear that this should take the form of a written policy document, which should be brought to the attention of the employee.

Technical / Security Measures - employers are required to safeguard against the unauthorised processing of data.

As often in data protection matters, this can be summarised as: do what you do only for good reason, do no more than is necessary for that reason, and keep data secure!

Summary

The privacy of private communications should be respected.

Where a telephone call is monitored and/or recorded according to a purpose specified in the Regulation, there is no need to tell external callers that calls will be monitored / recorded. Where such calls are recorded the author suggests it is good practice to bring this to the caller's attention, in order that the data is processed in a manner that is "fair".

Employees should be informed about the way in which data relating to them, including the monitoring and recording of telephone calls, is dealt with, and the aims of processing such data should be legitimate.

Written policies on what an employee is and is not allowed to do with provided communications systems are always best practice.