

## Privacy Issues



*"Vehicle telematics systems may be good news for fleet managers and insurance companies alike – but what about privacy and data collection laws? It's an issue that remains unresolved," says Steve Perham of Airmax.*

Vehicle telematics may be defined as the information-intensive applications enabled for vehicles by a combination of telecommunications and computing technology. Telematics by its nature requires the capture, storage, and exchange of sensor data to obtain remote services. Such data is likely to include personal, sensitive information, which requires proper handling to protect the driver's privacy.

After many a false start but seen by many as irresistible commercial sense, it's hardly surprising that the use of telematic technology systems is growing rapidly in the UK. Systems are widely used in a variety of applications including vehicle security, content supply and remote asset management. However, the ability to monitor and collect data on vehicle activity inevitably means monitoring and collecting data on driver activity, too, and here the technology can conceivably bring employers and service providers into conflict with the privacy requirements of the Human Rights Act and the Data Protection Act.

There are also other not insignificant matters for the employers to grapple with - such as duty of care and corporate manslaughter. For the enlightened employer duty of care requirements will take precedent over the Human Rights Act and the Data Protection Act. This is not unreasonable if you realise that a vehicle is also a place of work. So employers and employees alike have lots of matters and conflicting legalisation think about.

The Human Rights Act gives people a basic right to privacy, and although it is widely accepted that privacy at work is inevitably going to be compromised to some extent, the presence of an active location system outside normal working hours on a company vehicle being used privately by an employee - or a member of their family - could be regarded as a breach of human rights.

Meanwhile, the kind of data collection and distribution inevitably involved in remote vehicle asset management could also bring employers and those hosting the data into conflict with the Data Protection Act. This is dependant on what data is collected, how it is stored and used and shared. However with proper firewalls and secure web log-ins all issues relating to privacy can be dispelled. In the case of ALD Automotive's solution, Profleet2, the vehicle provider only retrieves accumulative mileage data and vehicle fault codes whilst the driver is free to securely subscribe to his own data with complete anonymity. Drivers wishing to take part in driver training and monitoring techniques or subscribe to Pay How You Drive (PHYD) Insurance schemes have to agree to the data being shared and as the benefits are potentially huge it is often given.

The potential for finding yourself on the wrong side of these laws was the subject of a strongly-worded warning by Birmingham-based solicitor David Faithful of Amery-Parkes in late 2002, but although there has been a lot of discussion since, the debate also maturing but little has been resolved.

There have been a number of disputes about privacy based on employment contracts, where telematics data has been used to dismiss or discipline employees. Often, this comes down to what is in the contract. Do drivers know the system is there? Are they aware specifically that they will be monitored and could be disciplined on the basis of it?



## PRIVACY ISSUES

Although no cases have yet gone to tribunal it must always pay for the employees to review their employment contracts and find out if it may be used for disciplinary or grievance procedures.

There is still no industry guidance on what data can be collected, how long it's kept for or how it's stored, the power to archive or delete sensitive data should rest with the owner of the data.

### **So whose data is it anyway?**

Well clearly out of hours driver data must belong to the driver.

Phil Jones, assistant commissioner at the Information Commissioner's office, stresses that it's not unreasonable for firms to want to manage their vehicles, and that where employees use their vehicles privately - service engineers' vans or company cars, for example - employers need to do three things: be transparent and up-front with the workforce about the use of the technology; ensure the data collected is appropriate and appropriately used; and provide an easy mechanism for turning off the system so that private usage remains private.

Even then, there are situations in which it might still be reasonable to monitor employees during non-working hours, states Jones - for example, if engineers were being paid for emergency call-outs at weekends and an employer wanted to see which engineer to send to an emergency based by their proximity to it.

It's very important, he suggests, for firms to understand their role from the data protection point of view. *"If companies who employ the technology are sensible in their approach and plan it and have a consultation process with drivers, so they know what the equipment is and what it's used for, then it should be possible to implement it within the laws."*

Until all the issues are tested in court, however, it seems nobody really knows for sure just where those legal limits really lie.

