

STATEMENT FROM PETER ERSKINE

Often companies are judged by what's most visible. This is why we make it a priority to ensure our approach to corporate responsibility is consistent and properly understood at every level within O2.

Corporate responsibility challenges conventional commercial thinking. It pushes companies to assess their impact beyond financial performance and to run themselves in a way that benefits society.

Our commercial success depends on how we behave as a company. Companies that win trust by being open and direct in all aspects of their business can build important links with the very people they depend on: their customers, employees, shareholders, suppliers, interest groups, local and national governments, regulators and investors.

From the outset we were determined to adopt the ethos of corporate responsibility and create a robust framework for our activities. We set ourselves the target of pursuing best-in-class corporate governance, ensuring that we weigh the social, environmental and ethical impacts of the business in managing risks to the Group.

We closely review and manage each of our risk areas; we listen to our customer and stakeholder views, and undertake proactive work around the issues.

We are sponsoring this online debate to stimulate views around the number of issues that surround privacy. Identify what the facts are, who is responsible and for what.

Fact: The mobile phone is personal. As soon as a phone leaves one of our shops it becomes unique to the customer, and over time more and more personal. In broad terms this happens in three ways. Firstly a record is built up of calls made, received, and places visited - physically and electronically. Secondly, most customers use their phones as a store of personal information - phone numbers, addresses, calendars, photos, notes and music are all kept on the handset. And thirdly, it becomes a store of identity - largely for the purposes of electronic commerce with applications such as being able to pay the London congestion charge by SMS.

This makes the mobile phone probably the most useful thing that most of us carry around with us. It provides the opportunity to communicate with voice, text and pictures; it provides a store of useful data, and it gives us the means to make personal transaction.

So in many ways our customers feel their mobile is a deeply personal item, something that contributes to their identity. Yet identity theft has become the UK's 'fastest growing crime' and the mobile industry a major target for those criminals seeking to trade off the back of stolen identities. Telefonica O2 Europe has not been complacent here. Working with the Government,

the National Consumer Council and industry bodies such as CIFAS, we have taken action to both strengthen protections for our customers and support for those customers who have been victims of such crime.

A consequence of this, of course, is the significant increase in the capacity to collect and process information about individuals, and the implications for personal privacy. We recognise this, as part of a general unease about both Government's ability to access personal communications, as well as the practices of commercial organisations.

This is clearly felt more broadly than just by mobile phone customers; internet users, store card holders, and digital TV viewers are as uneasily aware, as the pedestrian walking down the street under the eye of CCTV, of being watched. Nevertheless, the mobile is the most personal of these tools, and as network operators, we are keen to understand the concerns and desires of all those who have an interest. We are anxious to understand where our responsibilities lie in securing both people's safety as well as their liberty. This is why we are pleased to sponsor this on line debate.

Government has put in place a legislative framework which seeks to balance the collective security needs of the country, with the privacy needs of the individual. The Data Protection Acts, the Privacy and Electronic Communications Directive, the Anti-terrorism, Crime and Security Act, and the Regulation of Investigatory Powers Act together add up to a formidable regime. Our role is clearly to comply with this legislation which covers everything from communications intercepts, to cookies, from traffic data retention to spam. But as technologies develop, new issues emerge, and expectations both from customers, as well as law-enforcers are heightened.

Let's take a look at the current position in two areas: data retention and location based services.

Data retention:

The European Parliament's approved rules force telephone companies to retain call and internet records for use in anti-terror investigations. Records will be kept for up to two years under these measures, police will have access to information about calls, text messages and internet data, but not exact call content. The UK, which pressed European member states to back the rules, said that data was the "golden thread" in terrorist investigations.

The measures will require firms to store:

- Data that can trace fixed or mobile telephone calls
- Time and duration of calls
- Location of the mobile phone being called
- Details of connections made to the Internet
- Details, but not the content, of internet e-mail and internet telephony services

Significantly whilst the police need a warrant to access “content”, the same procedures do not exist for “traffic data”. The amount of information is potentially huge. Just to give some idea of scale, 4.4 billion messages were sent during March 2007 alone. Retaining this information would clearly be a major task, but the real problems would arise with any attempt to find useful data from that.

Our call records are currently retained for 12 months, but for billing purposes only. Text messages themselves, however, are currently only kept for a matter of minutes.

The Regulation of Investigatory Powers Act (RIPA) deals with Legal Interception (LI) and access to communications data and this legislation was enacted in January 2004. The main controversy in this area - and this is surely a matter for Parliament and not for network operators to resolve, is the extent to which public authorities over and above the police should have powers to intercept communications. Trading standards officers, fire brigades, local authorities have all sought powers.

Location Based Services

Mobile Phone location - Customers can use this technology to find out where they are, or to get localise information such as traffic reports or the location of the nearest cash machine.

From the outset in the design of these services we have been aware of the need for safeguards. Each O2 customer can opt out of location based activities. This is a simple procedure accessed by calling “1300” from the handset. When an individual tries to use a location service to track the movements of another mobile phone user, the service provider must obtain the consent of the locater before activating the service.

All the mobile operators got together to produce a code of practice that sets out such procedures.

We understand that commercial exploitation of Location Based Services is potentially contentious from a privacy point of view. My guess is that not many of us would welcome a fast food restaurant sending us a text message every time we got within 50 metres from one of their restaurants, but it is not for a mobile operator to say that this should not happen. Nevertheless, controls and safeguards need to be put in place; this is another form of spam, after all. But there may be other concerns. Where does the employee stand, who does not want to be tracked by his employer? Who has the right to consent to being tracked, the phone owner, perhaps a parent, or the phone user, perhaps a teenager?

Indeed, the challenges ahead are only going to be more complex. The latest generation of mobile technology, 3G, allows for great flows of data across our network, as well as more accurate location fixing.

Technology such as Bluetooth, which enables PCs, PDAs and mobiles to communicate wirelessly across short distances - both directly with each other, or to access other networks using WiFi, open the door to new possibilities. These technologies will help with policing and evidence gathering over the current technologies, but with these possibilities comes the potential for abuse by those with criminal or malevolent intent. Even if technological solutions existed, how are these to be controlled without compromising people's privacy? Do we need to make a distinction between phone crime - paedophiles, for example, using the technology to groom children, and general criminal activity?

Of course, technical measures will only ever form part of the solution. With increasing incidences of criminals and the press seeking to 'socially engineer' access to our information it is imperative that customer service training and education form a key part of any defence. That is why O2 UK held a 'Blagging Week' in October last year, to ensure our call centre staff are fully aware of the latest social engineering practices.

Interest groups, parts of government, and even individuals make numerous calls on us to exploit our network and its information for a number of reasons. Of course it is not just one piece of technology, or one piece of legislation that defines the issue, but the combinations, and their applications. Some, for example, suggest we should not make location data available for commercial purposes, others suggest that location data is valuable to people such as parents seeking to know where their children are.

It is for government and the authorities to determine their own roles. To conclude, what role is there for a phone company? We exist to provide voice, text and data services to customers. The information that we currently hold is from systems designed for billing purposes. The location data is a by-product of the technology and its collection and retention is not our core business. While it is right that we should cooperate with law enforcement agencies, arguably it is not our duty to go out of our way to accumulate data that we don't need in order to satisfy the potential requirements of the police, trading standards officers and so on. Or should we?