

Data Capacity Limitations and their effect on internet usage

If you phone Australia for an hour long chat with Aunty Doris, you know that you will be paying for the privilege. On the other hand, if you're blithely using the internet to download the next episode of 'Lost', you may be in for a nasty surprise when your next bill plumps onto the door mat (or in tray as the case may be).

We may all like surprises, but not when it comes to paying our bills. The essence of keeping customers happy is to ensure that they clearly understand what they are spending on the service they subscribe to. Broadband providers who fail to learn this lesson will quickly lose their market share to providers more attuned to the needs of their consumers.

There is going to be a huge slice of the population whose use of broadband will not extend beyond sending the odd photo by email attachment and who will never exceed their monthly data cap. Others (and you know who you are) are in the fast line on the information superhighway. You wouldn't expect a turbo-charged Reliant Robin, and the same goes for your choice of broadband. In other words you pay for what you get. If you want a service that's sleek and mean, that's what you should go out and find.

That being said, if you shop around you can expect to pick some good broadband deals. We should be prepared to change our internet provider regularly. If providers do have to apply data caps, then arguably they should at least warn you when you exceed your cap. If the cap doesn't fit, don't wear it.

Email Security and Usage

Data Security:

If your job is to maintain the security and integrity of your organisation's network, a detailed knowledge of the Data Protection Act and related legislation is a boring but necessary part of the job for many of my clients.

Legislation can really only recommend the basic principles and the world of IT will inevitably develop more quickly than the legislation underpinning it. The challenge for network security specialists developing new systems and solutions is to work within the letter and spirit of the legislative framework.

For most businesses regulatory compliance is inextricably linked to the commercial need to maintain secure networks. For example, if a credit card company failed to maintain network security, it would expose itself to the major fraud and legal claims which could cost millions of pounds.

Storage of Data:

The importance of backing up data must have been brought home to many of us by the experiences of businesses large and small in New Orleans, many of which no doubt will have suffered a devastating loss of data following Hurricane Katrina.

If anyone has any doubt about the importance of backing up data, it's worth bearing in mind the following points from a legal perspective:

As a general rule legal actions may be brought within six years of the act or omission complained of. Liability can attract not only to the company itself but to the directors or even in some cases the main share holders.

Under the DPA, 'personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes of which they are processed'. There's also an obligation to keep the personal data up to date. In other-words you should have a rigorous system in place to ensure for example that your ancient data files only contain relevant, adequate and up to date personal information.

The DPA states that "appropriate technical and organizational measures shall be taken" to safeguard personal data. This is something that many businesses abjectly fail to do. As a result, credit card numbers, membership lists and other personal data have occasionally become publicly accessible on the web. From a commercial point of view, lose that data, and you may not have a business at all.

Pay Per Click Campaign - Fraud Abundant

"Most businesses shelling out their hard-earned marketing budget on a pay per click (PPC) campaign want to know that they can rely on the statistics they are provided with. After all most newspaper and magazine circulations are independently audited. However you may only have someone else's word to take for it on a PPC campaign.

An advertiser's claim that 'we regularly get 10,000 hits per week' for example could amount to negligent or fraudulent misrepresentation, and in any case may well not tell the whole story. But how will you ever know?

If possible, such claims should be independently audited. If not then before investing your money you will need a clear understanding of how the statistics are collated and what they actually mean. The more money you are investing, the more care and attention you should take over the wording of the contract that you enter into and you should consider implementing a contractual mechanism for resolving any disputes effectively.

In the same way that dodgy pop-bands may tour the Record Shops buying their own single in order to boost their chart rating, the number of clicks may be fraudulently boosted to your cost. You may therefore want to be able to check whether repeated clicks have come from the same place to see if this is happening.

We all know the phrase 'Lies, damn lies and statistics'. Even when the campaign provider is entirely honest, you may still walk away dissatisfied by the campaign, without necessarily any legal recourse. It's worth taking up references from other clients who have used the same PPC campaign provider, and see how happy they were with it and how it worked for them."

Financial Marketing - Opting in & out

Whilst voluntary codes of conduct may exist, there is no statutory provision for unsolicited mail in the UK. However when it comes to email it's a different matter. Under UK law (Reg 22 of the 'The Privacy and Electronic Communications (EC Directive) Regulations 2003' (<http://www.legislation.hmsso.gov.uk/si/si2003/20032426.htm>)) you can only send unsolicited marketing emails to an individual subscriber unless he has previously consented to receive it, or:

- You have already sold something to the recipient, *and*
- You are marketing a similar product, *and*
- You include an 'unsubscribe' option in each email.

Emails which conceal the identity of the sender are not permitted under the UK provisions. Similar regulations apply in other EU countries.

Recipients of spam can 'bring proceedings for compensation'. The Information Commissioner can assist, but unlike provisions in other EU countries such as Italy, these regulations are entirely without teeth.

For most legitimate businesses, the fear of causing ill-will is a stronger incentive than any legislative provision not to spam. 'Do as you would be done by' is a good principle on which to

proceed. 'Opt in' marketing schemes will be much more effective than 'opt out' ones. A marketing campaign that alienates consumers is clearly a non-starter.

If you plan to hire an external marketing firm, ask for their Data Protection and Consumer Privacy Policy. If they don't have one, take a good hard look at whether you still want to work with them.

Suing Bad Developers - Is it really worthwhile?

Ok. So you've employed a developer. He makes a pig's ear of the development work you hired him to do. Your client pulls out claiming shoddy security and sues you for negligence. You mention to the developer in question that you are thoroughly underwhelmed by his contribution to the mess you find yourself in.

If you follow a fair procedure, you may well be able to dismiss him for lack of ability. However it's fairly unusual for employers to go a step further and sue their employee for negligence or breach of contract. The point is though that there is no reason in law why you should not.

That being said there are practical reasons why this tends not to happen. Developers, whether employees or contractors, seldom work in isolation and generally work as part of a team. In other words, evidentially it's often hard to pin the blame on a particular person. IT demands a high degree of innovation. If your employees (or contractors for that matter) are scared witless at the prospect of being sued simply for doing their job, you won't keep them for very long. The few that you do retain will be very very careful, but their creativity will suffer as a result.

If a litigation culture is encouraged, you will drive developers into the arms of professional indemnity insurers, and you'll simply force up your costs when you may do better taking out insurance yourself. There is little wisdom in suing someone who is unable to pay the award and legal costs even if you do win.

If you don't have systems in place to prevent rogue developers, then in the same way that Barings Bank failed to stop rogue trader Nick Leason, you will be failing in your *own* job. Don't just pass the buck.