



# analysis

## Private Email at Work

### Summary

**Companies are being forced to deal with the problems caused by employees using the company's email systems for private purposes because of increased regulation and requirements to archive email and simply because so much of their business goes through email nowadays**

### Background

The use of company resources whilst at work is not a new problem. It used to be the case that telephone use was restricted but as more and more people got their own office phone most companies ran a policy of allowing "reasonable" use. This meant, for example, no transatlantic phone calls for private purposes! A large proportion of staff now have their own pcs and with them Internet access. For security and other reasons companies will try and monitor and restrict web browsing by employees and there are tools to allow this that will run on corporate networks. Now the issue of private use of email is becoming more important for a number of reasons. In the USA just over half of employers review and retain employees email messages.<sup>1</sup>

In the UK following in the wake of the budget announcement that the scheme that subsidised the purchase of computers by employers for employees was to be scrapped there was speculation that private use of computers at work would be liable to be taxed.<sup>3</sup>

### Email at work

Many companies have had a relaxed attitude to people sending private email from their companies email accounts - i.e. with the company's domain as part of the email address. In the past this has caused problems and issues have been raised regarding privacy of employee email and clearly the issue arises of whether such emails could be construed in some circumstances as being on behalf of the company rather than private email. One advantage of taking a relaxed attitude is that at least the company can make sure that email coming from its own or employer contracted hosted email services has been virus checked before it gets onto the users pc.

However in the last year matters have taken another turn. Companies are increasingly realising that they need to not only keep back up copies of emails but to archive them. In other words they need to store emails in such a way that they can be stored and retrieved and that they cannot be tampered with. Hence it is not sufficient to rely on emails being stored on individual machines with the responsibility lying with the employee. In fact clearly employees can alter information on their own pc (e.g. delete emails) and this is not acceptable in the current climate. What happens when they leave for example or change jobs or just get a new pc?

Archiving solves these problems but accentuates the problem of private vs. company emails. Do you really want to have all those private emails and what are the privacy issues nowadays? How happy is the employee that all their email is being stored for years and easily retrievable by the employer?

An analysis of the legal position makes clear that any email from a companies email account is almost certainly to be treated as an official communication from that organisation. <sup>4</sup> In fact company email is more akin to an employee using company headed notepaper for private correspondence and this is something that an employer would treat very seriously indeed. The whole issue of disclaimers and signatures is covered in more detail in another SMS Analysis paper - "Disclaimers and Signatures".

Finally if the plan to tax employees for private use comes to fruition employees may even be forced to differentiate anyway between what is a private and company email in order that tax could be accessed. This would be easier to achieve if the employee did not use the employers email system at all but had an alternative means of accessing private email at work.

#### What to do about the problem?

There are a number of potential solutions:

The simplest solution is just to ban the use of company email facilities for private messages. However this would require the monitoring of emails and require disciplinary procedures being set up.

- Combined with a ban employees could be told that they could use outside email services. Some are free such as hotmail or gmail but these would still require that the corporate network allows access to the webmail interfaces for these services. Many employees would want to use more sophisticated services allowing them to access their email at home and whilst on the move such as subscribing to email hosting companies offering Microsoft Exchange Server or in the UNIX world Zimbra or Scalix. Such an approach would increase the risk of viruses being introduced to the company network.
- A further solution would be for the employee to subsidise email services with a hosting provider for employees. This would have the advantage of just needing to allow access to a single server from the corporate network and would reduce the temptation for private use of company email (especially if it was for a more sophisticated service as mentioned above). In fact such a move would suit the situation where the users are Blackberry addicts because they could move to getting "push" email onto their Windows Mobile 5 devices. One criteria for choosing the supplier would be that they include virus and spam checking with their accounts. The subsidy could be time limited or on a percentage basis. The employee would take over paying for the account if he left saving him considerable hassle. \*

We have just looked at things from the employer point of view. But how do employees react to knowing that all their email is being saved and scanned and stored for up to seven years (or more dependent on the situation). It is probably bad enough to realise that emails that were

sent on company business (or internally) could come back to haunt them later but surely worse that all private emails are similarly being stored.

*\* This solution gives the employee PIE (Provider Independent Email) - this means an email service from a specialised email hosting company using a personalised domain. If the ISP that the employee uses at home is changed their email address remains the same.*

## Conclusion

Companies need to have a policy on the private use of email that safeguards their networks and provides an alternative for employees that they will really make use of. They need to avoid any ambiguity regarding what is sent out in their name. Tax plans may make it necessary for employees to have separate email facilities from those of their employers.

### 1) Privacy Rights Clearing House:

<http://www.privacyrights.org/fs/fs7-work.htm> - a USA Website that states quite clearly that if it goes through the employers equipment it is not private.

### 2) A general review of On-Line rights at work:

<http://www.andrewbibby.com/socialpartners/onlinerights.html>

### 3) Tax on staff e-mail to friends:

<http://business.timesonline.co.uk/article/0,,16849-2159286,00.html>

### 4) Discussion of the legal position particularly provenance of email:

[http://www.weblaw.co.uk/art\\_faqs.php](http://www.weblaw.co.uk/art_faqs.php)

### 5) Email resource site:

<http://www.allaboutemail.info>