Chapter 8

E-mail marketing challenges and innovation

CHAPTER AT A GLANCE

Overview

This chapter looks at issues that will affect the future of e-mail marketing, many of which are significant already. They include challenges such as achieving deliverability, given the rise of spam, and attaining the right balance between frequency and return on investment. There are also technological innovations, including wireless access devices such as PDAs and mobiles, and the new opportunities for rich media, such as video streaming provided by increased bandwith. The impact of Really Simple Syndication (RSS) on e-mail marketing is also covered.

Chapter objectives

By the end of this chapter you will be able to:

- assess different approaches being developed to control spam.
- evaluate the relevance of rich media e-mails.
- identify the options for e-mail using wireless access devices.
- assess the role of RSS in the future.

Chapter structure

- Improving deliverability
- Touch frequency
- Rich media e-mails
- Messaging through mobile or wireless access devices
- Really Simple Syndication
- References
- Web links

IMPROVING DELIVERABILITY

Newmediazero (2002) reported that, according to a new Forrester report, the 'spam flood will drown E-mail marketing'. Forrester predicted that all attempts by ISPs to filter spam and efforts by governments to legislate against spam would be ineffectual. Four years later, we can see that the gloom of this prediction has not transpired. Response data showing e-mail responsiveness measured by clickthrough of e-mails delivered have remained similar despite the volume of spam increasing to over 90 per cent of all messages, according to Messagelabs. This is because consumers seem to be good at identifying permission-based e-mail in their inbox – the permission marketing concept works!

What has transpired, though, is that e-mail marketers have had to work much harder to get their e-mails delivered, given the increase in efforts by ISPs and web-email companies to reduce the amount of spam arriving in their end-users inboxes. This results in '*false positives*', where permission-based e-mails may be bounced or placed into junk-mail boxes, or simply deleted if the receiving system assesses that they are spam. Although deliverability rates remain high, it may be that some e-mails which appear to be delivered do not get through to their recipients.

Know your enemy – what can lead to you being identified as a false positive?

Spammers work hard to understand why their messages are not read and find methods to avoid being blocked. Here, legitimate e-mail marketers are much like the spammer, since they and their suppliers also need to understand what is stopping their messages getting through and identify solutions to this. There are four general points where spam or legitimate permission-based e-mail is identified, and which can stop e-mail being read by the recipient:

1. *Inbox identification by the user*. The simplest way that spam is identified is by the recipient; if it looks like spam from the header, it will be quickly removed using the delete button. Alternatively, recipients can report spam to their anti-spam software and, if enough people do this, there is the danger that may be added to a blacklist.
2. *Software filtering*. E-mail can be identified as having the characteristics of spam by anti-spam software, which may run at a variety of locations – at the ISP, a third-party mail-scanning service, a company firewall or mail server, at a web-based e-mail service server or on the end-user's computer.
3. *Domain blocking*. Here, the domain from which the e-mails are broadcast is blocked since its IP address is deemed to be a known source of spam.
4. *Sender authentication systems*. Here, the recipient's system or administrator identifies that the e-mail has not been sent from a recognized broadcaster.

Let's now look at these in a little more detail.

Inbox identification

An e-mail will look like spam if recipients don't recognize the sender – i.e. it is not a company or product known to them as indicated by the From, subject line or preview pane. If it is not clear from the subject line, a preview of the text in the e-mail will usually show whether or not it is relevant. For an in-house e-mail list you must therefore use the company or brand name in the From address, or in some cases (like an e-newsletter where the name of the e-newsletter is in the From address) use the name of the company or brand in the subject line.

For campaigns using rented lists or co-branded with a partner, it is more tricky. Many companies concatenate both list owner and the brand being promoted in the From as in 'Freeserve-Accucard', but since this may get truncated it is perhaps better to put the brand in the subject line.

Another vital step to avoid being identified as spam by the recipient is to use copy within the message that explains that the message is *not* spam. This is commonly headed as a 'statement of origination' or, more informally, 'Why am I receiving this e-mail?' This should explain either that the recipient has opted in, ideally with the place and time of opt-in, or that the e-mail has been sent because the recipient is an existing customer. You should also explain that the message is within the law of the country.

For e-mail campaigns using rented or shared lists, it is essential that the statement of origination is clear, typically at or near the top of the message. For house-list campaigns it is still useful to have a statement of origin, but is probably best at the foot of the message.

It is also best practice to invite the recipient to add the e-mail to the '*safe senders list*'. Some e-mail providers have set up pages to explain how the end-user can do this for different web mail and desktop mail packages. For example, Tesco has this message at the top of its e-mail, in a discreet colour:

> ***To ensure that your Tesco e-mails get to your inbox, please add mailto:online@tesco.co.uk to your e-mail Address Book or Safe List. For instructions, click here.***

Software filtering

There are now many techniques that are used by different types of anti-spam software to identify spam. We will now review some of the most common ones, which are often combined in a single anti-spam tool, and describe the type of steps that marketers can take to avoid being wrongly identified as spam.

Keyword and key phrase filters

First-generation anti-spam software uses a simple 'look-up' table of words that are commonly used by spammers, such as 'viagra', 'sex', 'over 18' or 'free'. If these words are contained in either the message header or the body, then it is deleted or assigned to a junk-mail folder.

Such words do not present a problem to most companies, but what if your company is in Sussex, or you are a bank that by law has to say that your product is only available to those who are over 18? Or maybe you are offering a free trial. In these cases, one alternative may be to use these 'naughty words' as part of graphics embedded within the e-mail, which will not be recognized by most filters. Of course, the spammers use variants of words, such as 'v'iagra' or 'vlagra'.

Do not be overly concerned by using words such as 'free' in the subject line – I have seen tests where such e-mails pull a higher response than more subtle approaches. The reason is that many spam filters now use a more sophisticated approach . . .

Message rating filters

Second-generation anti-spam software uses a scoring system where different keywords and different phrases score different points – for example, 'free' might score 2 points and 'sex' 10 points. If the e-mail is rated over 15 points, it will be classified as spam. Some programs now have Bayesian filters, which use a mathematical model to learn the characteristics of spam and watch for patterns typical of spam. You may have noticed gobbledy-gook phrases at the bottom of some spam messages; these are used to overcome such an approach. An example of a spam rating available from the ESP Email Reaction (www.emailreaction.com), based on the Spam Assassin rating, is shown below. Such facilities are available to help you assess your e-mail for 'spamminess' before you send it. You can see that, in this case, some factors are set to 0, but for some firewalls these could be given higher values.

Words likely to trigger content filters

These words may trigger some content filters: viagra.

HTML and technical issues

Content analysis details: (4.4 points, 5.0 required)

pts	rule name	description
0.0	SUB_FREE_OFFER	Subject starts with 'Free'
1.8	SUBJECT_DRUG_GAP_VIA	Subject contains a gappy version of 'viagra'
0.5	TO_ADDRESS_EQ_REAL	To: repeats address as real name
0.2	HTML_IMAGE_RATIO_04	BODY: HTML has a low ratio of text to image area
1.5	HTML_IMAGE_ONLY_12	BODY: HTML: images with 800–1200 bytes of words
0.0	HTML_WEB_BUGS	BODY: Image tag intended to identify you
0.2	HTML_FONT_BIG	BODY: HTML tag for a big font size
0.0	HTML_TITLE_EMPTY	BODY: HTML title contains no text
0.0	DRUGS_ERECTILE	Refers to an erectile drug
0.1	MIME_BOUND_NEXTPART	Spam tool pattern in MIME boundary

These are some tips from David Hughes of Email Vision (www.emailvision.com) on how to reduce problems of content filtering:

- Avoid or minimize spam phrases, particularly in subject lines
- Minimize use of capitalization
- Keep HTML simple
- Carefully word your unsubscribe method so it doesn't look like that commonly used by spammers; don't mention spam compliance as such
- Don't overuse large fonts and garish colours
- Newsletters are less likely to be blocked, so show clearly that you are a newsletter
- Avoid the message being too small – spammers and phishers today often find that a single embedded image with their message in it gets through the filters, particularly if it has a paragraph of legitimate newsletter-like text at the bottom of the e-mail.

Messages are also blocked if the original From address has been masked, so it is important for legitimate marketers not to do this. If your e-mail management system doesn't contain these spam rating features, then you can try using this service (which is currently free): Lyris Content checker (http://www.lyris.com/contentchecker).

Blacklists

Blacklists are lists of known spammers, such as those reported to Spamhaus Project (www.spamhaus.com) or SpamCop (www.spamcop.net). If a recipient is on the blacklist, it is deleted or put in the junk-mail folder. Blacklists are often used in conjunction with filters to block e-mails. One of the most widely used systems is that developed by Brightmail (www.brightmail.com), which uses a global network of e-mail addresses set up to trap and identify spam. Brightmail is increasingly used by ISPs such as BT to block spam.

Blacklists are also used by many types of anti-spam software, such as the two most popular – McAfee SpamKiller and Norton AntiSpam.

It is unlikely that legitimate marketers will be placed on these, but it may be worth checking. However, there is an argument for companies who send out a lot of consumer e-mail to test whether messages pass through the main filters. Filtering used by major ISPs such as BT, AOL and Freeserve, and also web-based e-mail services such as Hotmail and Yahoo!Mail, should also be tested.

Using seed addresses at some of these accounts can help, but you may be missing some. Email Monitor (www.emailmonitor.co.uk) estimates that 99 per cent of e-mails in the UK are ultimately delivered through 20 ISPs. It offers a tool, known as MailBox Monitor, which is configured with addresses at these 20 ISPs in order to test for blocking due to blacklists or the different filters described above. It also has a tool known as Message Check which tests an e-mail address, before sending, against the main filters.

Lyris EmailAdvisor (http://www.lyris.com/products/emailadvisor) also includes a blacklist monitor and deliverability service. Blacklist monitor (http://www.blacklistmonitor.com) is a low-cost service, with a free trial that enables you to see whether the IP address of your e-mail marketing broadcaster is blacklisted.

Whitelists

An organization whitelist is a list of *bona fide* e-mail addresses that are likely to want to contact people within an organization. It will include all employees, partners, customers and suppliers who have obtained opt-in from employees to receive e-mail. A personal whitelist is one created by the user of e-mail software, listing message senders he or she is happy to receive e-mail from.

The organization whitelist approach has not been adopted widely because it is difficult to set up, but it probably offers the best opportunity for the future. The personal whitelist feature is becoming more common in anti-spam software, and is now built into Outlook or the popular Qurb (www.qurb.com) service, which guarantees to ‘block 100% of Spam’!

However, there is little action marketers can use other than recommending that their company be put on the recipient’s whitelist. Some e-mail recipients may use such tools rather than opting out.

Challenge/response authentication

In this approach, if an e-mail is sent from someone who is not on your whitelist (or is possibly on your blacklist), a message is automatically sent asking the sender to provide manual confirmation or authentication of identity by following a link from a challenge e-mail that requires a response. This approach is available as part of anti-spam solutions from companies such as Spam Interceptor (http://si20.com) and SpamBully for Outlook (www.spambully.com). The theory is that spammers are not going to be able to respond; the problem is that permission marketers will not be able to either. Fortunately, it seems that this approach is not widespread . . . yet.

'Peer-to-peer' blocking services

These take advantage of the fact that humans are good at identifying spam; when they do so they then notify a central server, which keeps an index of all spam. SPAMNet from CloudMark (www.cloudmark.com) requires users to identify spam by pressing a 'Block' button in Microsoft Outlook, which then updates a central server so that when others download the same message at a later time it is automatically identified as spam. I have used this service and it works effectively, but I have noticed a problem in that legitimate e-mails I have opted in to can be classified as spam by other users. They can be marked as legitimate, however, by the recipient.

Domain blocking

ISPs or firewalls can block individual domains or web IP addresses that are known sources of spam, or where the pattern of broadcast suggests spamming. This approach is intended to trap known spammers who hijack servers and send out a large number of e-mails. However, it can lead to legitimate e-mail marketers being blocked, particularly if their e-mail platform is co-hosted by a machine that has been hijacked. This may also be a problem if you send out a large number of e-mails in a short period, such as when your e-mail broadcaster or in-house system sends more than 10 000–15 000 e-mails per hour. Web-based e-mail vendors such as Hotmail, Yahoo!Mail or AOL may blacklist companies who broadcast too many.

One solution is to send out the e-mails over a longer period or 'throttle back' the rate at which e-mails are sent. However, it is difficult to know which ISPs are blocking your domain.

Also check whether your broadcaster has a deliverability monitoring tool. One of the first tools developed was IP Block Alert, also from IPT Limited's Email Monitor (www.emailmonitor.co.uk). Most of the major e-mail broadcasters now offer this facility.

Sender authentication systems

These approaches seek to prove the sender of the e-mail is legitimate – that senders are who they say they are. The SMTP standard used for e-mail allows any computer user to send e-mail claiming to be from anyone, so its easy for spammers to send e-mails from forged addresses. Authentication uses different methods, which require senders to establish who they are. There are several approaches.

Reverse DNS look up

DNS stands for Domain Name System – it's how computers find each other on the Internet, a bit like the Yellow Pages. The DNS is a mapping of the IP address (e.g. 64.233.179.104) that uniquely identifies each computer attached to the Internet with its physical addresses. For example, the IP address given above maps to the domain google.com.

Many ISPs now perform what is known as reverse DNS to check that the e-mail sender has a valid domain with a published DNS record. This is only possible for servers with a static IP address, such as legitimate ESPs. Spammers may be using software installed on infected end-user machines known as 'zombies', which typically have dynamic IP addresses (they change every time the user logs on).

Sender Policy Framework (SPF)/sender ID

In 2004, there was an announcement of intent for international cooperation by governments to encourage ISPs to create an effective infrastructure to limit spam. Initially this was to focus on reducing the ease with which spammers can spoof or mask their real address in e-mail headers by replacing it with another domain name. This would prevent spammers using common domain names, such as Yahoo.com or Hotmail.com. However, some believe it will not prevent spoofing of less well-known names. Providers such as Sendmail (www.sendmail.com) are now developing 'sender authentication technology', which allows organizations to verify the source of a message before accepting it by automatically checking if an e-mail comes from where it claims it does.

Microsoft announced its Sender ID technology in 2004, but the standard with which it is linked (Sender Policy Framework (SPF, http://www.openspf.org) is better known and supported by more open-source server providers. It is due to be ratified by the Internet standards body (IETF). Both techniques are based on the broadcasting domain publishing a DNS that shows it is a genuine sender. This verification is automatically performed by the ISP or recipient's mail server before the e-mail message is delivered to the user.

When the e-mail is received, the receiving mail server checks the domain indicated in the e-mail header against that published in the public DNS (i.e. against a registered list of servers that the domain owner has authorized to send e-mail). As Figure 8.1 shows, if the two do not match, the e-mail is not transmitted. See http://en.wikipedia.org/wiki/Sender_Policy_Framework for more details.

Domain Keys

Yahoo! Domain Keys also aims to combat domain spoofing and to assist in tracing spammers. It will generally be deployed alongside SPF. The approach used is different. When the e-mail is sent from a domain, it is encrypted using a private key that can only be used on the domain (effectively a digital signature). The receiving SMTP server then checks this digital signature against the public key for that domain, and if it is an authenticated, genuine sender they will be same. This approach has so far been implemented on Yahoo! Spam Guard, BT Openworld and Gmail.

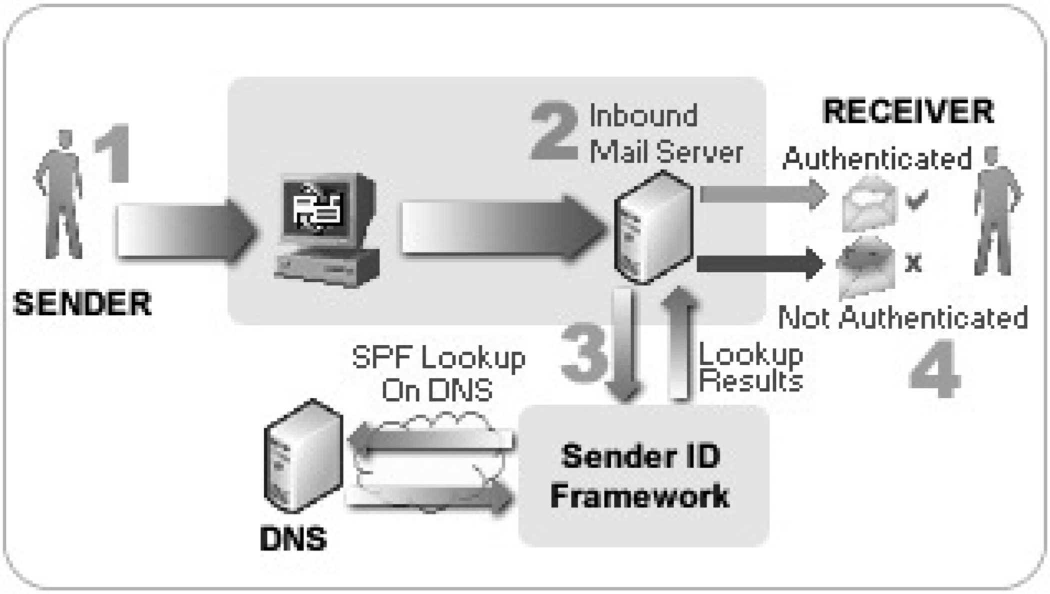

Figure 8.1 Microsoft Sender ID

Sender-warranted e-mail

Sender-warranted e-mail use some type of watermark to identify legitimate e-mail. Habeas (www.habeas.com) is one company that has promoted this approach. This is a great example of lateral thinking. The e-mail message contains a defined signature which is based on a small *haiku* poem – for example, the footer might contain 'X-HABEAS-SWE1-Winter Into Spring'. E-mail marketers who use the Habeas service have the right to include these identifiers in the foot of their message. Since Habeas has an agreement with the major ISPs, such as AOL, and anti-spam services, such as Message Labs, such messages are never classified as spam because they are from a trusted sender.

Of course, some spammers have started using the Habeas codes within their e-mails, but two prosecutions have been brought against them.

A similar approach is the concept of a 'bonded sender', developed by Ironport (www.bondedsender.com). Senders of opt-in e-mail post a financial bond to prove they are a reputable company. Senders of spam would not be able to afford to pay the bond. Recipients who feel they have received an unsolicited email from a Bonded Sender can complain to their ISP, IT manager or IronPort, and a financial charge is debited from the bond.

Pay per e-mail

An additional component of future approaches could be to charge a tiny amount for each e-mail sent, particularly where multiple messages are sent. This would eliminate the economic incentive for spammers, particularly if they could not hide the source address. What is of

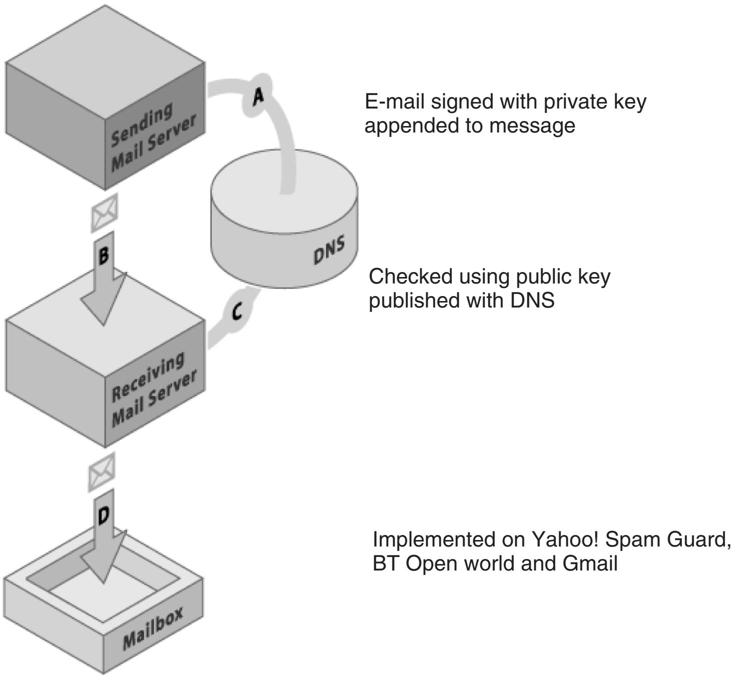
Sending Mail Server
A
E-mail signed with private key appended to message
DNS
B
Checked using public key published with DNS
C
Receiving Mail Server
D
Implemented on Yahoo! Spam Guard, BT Open world and Gmail
Mailbox

Figure 8.2 Yahoo Domain Keys

more concern is proposals to charge large-volume e-mail broadcasters. Although companies using third-party broadcasting services are already paying between 0.5 p and 10 p per message, companies broadcasting their own e-mails would also see an increase in costs. However, any small increase in price per message may be able to be borne by companies if current response rates prevail. Indeed, one argument is that with less spam, response rates will increase.

E-MAIL MARKETING INSIGHT

Review the authentication used in the broadcast of e-mail messages from your internal servers or those of your ESP. Best practice is to use Sender Policy Framework and Domain Keys as a minimum.

Given that there are so many methods used by different web-mail providers and ISPs for countering spam which may also block legitimate e-mails, it is important, particularly for large-volume senders, to test to see whether particular providers are blocking your areas. A recent post on E-consultancy (www.e-consultancy.com) highlighted how a B2C company was sending hundreds of thousands of e-mails to MSN/Hotmail but none were getting through. Worst still, there was no notification of this – it is not practical or desirable for the receiving mail server to send back hundreds of bounces; they are simply discarded. How, then, can you find out if this is happening? Well, it's simple if you look. You can simply report on open rates and click rates by provider – you would see in this case that there were no opens or clicks from people on your list with Hotmail addresses.

E-MAIL MARKETING INSIGHT

Ensure you check for deliverability problems by reporting hard bounces and also opens and clicks by the main ISPs.

TOUCH FREQUENCY

A further challenge suggested by the Forrester research, and referred to at the start of the chapter, is achieving the delicate balance between frequency of campaigns and response. As suggested in Chapter 4, finding the right touch strategy is important to maximize the value from an e-mail list while at the same time not annoying customers or losing response owing to too high a volume of e-mail.

Consider the example where a retailer is broadcasting a fortnightly e-mail and finds that, through running a test, increasing the frequency to weekly also increases sales. It then rolls out at this frequency to the entire list, but over time the negative impact is felt with decreased sales, increased unsubscribes and a negative perception from list members. What approaches can be used to resolve this dilemma? Here are some suggestions:

1. Offer more customer choice by offering communications preferences – enable customers to tailor the type and frequency of communications received. Amazon provides this facility, although not at opt-in (users are opted into all communications by default); it is available to customers if they feel they are receiving too many messages. Contrast this with other e-retailers, where the only option is all or nothing.
2. Customers who are responsive to e-mail must be monitored at a more granular level than the whole list. Customer responsiveness can be assessed relative to typical values, and customers who are less responsive (for example, if they are not regularly clicking through on the e-mail) should be e-mailed less frequently. More periodic e-mails with stronger offers may have a stronger response.
3. Increase the relevance of messages by matching them with customer intent – i.e. a sense and respond approach where e-mails are sent in response to customers at different stages of the lifecycle, or when they are visiting the web site unprompted by an e-mail.
4. As you use more advanced targeting, it becomes increasingly difficult to monitor the number of e-mails received by customers; will vary according to different selects against the database. Producing a touch frequency plot such as that shown in Figure 8.3 can help to assess whether some customers are being e-mailed too often or not often enough.
5. Put limits on e-mail frequency, such as minimum or maximum e-mails in a period, as described in Chapter 4.

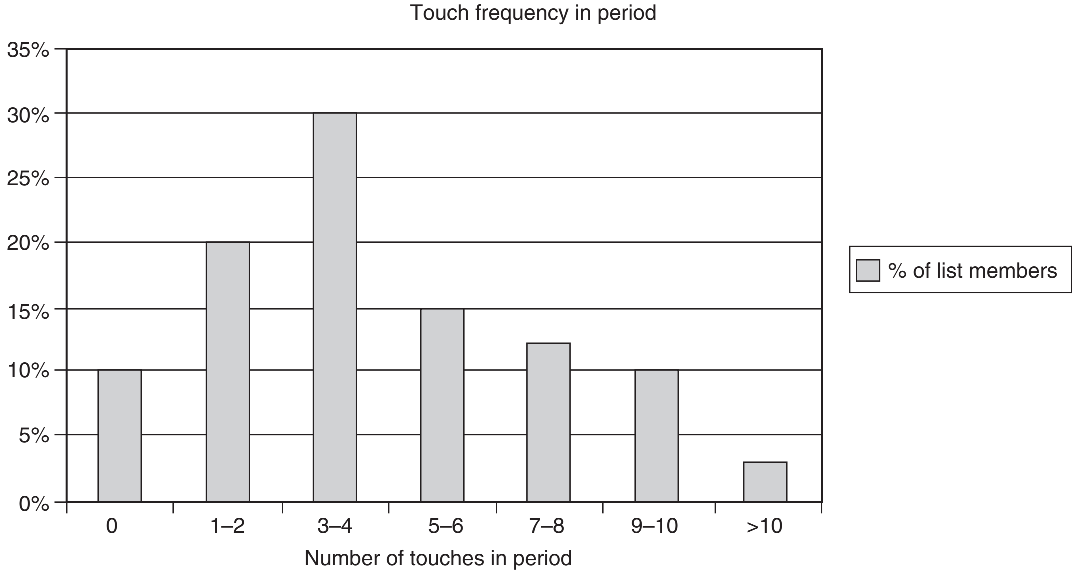

Figure 8.3 E-mail touch frequency plot

RICH MEDIA E-MAILS

Rich media e-mails go one step beyond the use of static or animated graphics in HTML e-mails, and give a richer experience through more complex animation, video and/or sound. Some refer to HTML as rich media, but more commonly the term is used to refer to e-mails with more dynamic or interactive content. A video can be streamed when the user opens the e-mail, or the message displayed in the preview pane and the video downloaded and displayed in real time – for example, Trailermail (www.trailermail.co.uk) is used to provide video trailers for movie companies. Alternatively, Flash animations can be integrated into the e-mail.

Many brands have experimented with rich media e-mail, but they don't seem to be increasing in popularity. There are several potential reasons why they have not been used more widely:

- E-mail, as with other digital media, tends to support impulsive behaviour – we don't want to wait for downloads unless the download is compelling
- Many corporate firewalls can block streaming media and, because of the high at work usage of e-mail, companies cannot risk reducing the visibility of their message
- Again in the corporate setting, e-mail recipients often won't want to be seen listening to or viewing a video clip by their boss, unless they control the media and turn on audio
- There is not a clear relationship between the incremental cost of rich media and the returns generated either through response or uplifts in brand awareness and favourability.

Owing to the technical issues of delivering rich media within the e-mail, increasingly companies are using an approach where the message directs the viewer to a web site to download or stream a clip. Of course, this means that the e-mail has less impact itself. If rich media is used in e-mail, it is more likely to be relatively simple – perhaps a flash animation – and is used to complement a text or static image-based message which will be effective even if the rich media element doesn't download.

E-MAIL MARKETING EXCELLENCE

One example of a successful rich-media e-mail innovator inbox (www.inbox.co.uk) is given by BUPA, where a rich media message was used to target personnel managers in organizations with more than 500 employees. The message was offering health cover to employees through a company scheme. The creative consisted of a personalized video showing the time savings that companies could potentially make. The results were:

Open rate	52%
Click rate of open	21%
Request call of open	8%
Conversion to appointment	18%

During the campaign, the company monitored which recipients opened the e-mail and these were then followed up by phone.

MESSAGING THROUGH MOBILE OR WIRELESS ACCESS DEVICES

Mobile technologies are not new; it has been possible for many years to access the Internet for e-mail using a laptop connected via a modem. With the ongoing convergence of devices, we are now seeing a range of hybrid devices combining PDA features such as calendar, address list, task list and office tools with phone features.

The importance of mobile access devices for messaging in the future is evident from Figure 8.4. This shows that, in the UK, the usage of mobile phones far exceeds that of the fixed Internet. This pattern is repeated throughout the world. What does this mean for e-mail marketing? First and foremost, messaging to mobile devices offers greater reach than Internet-based e-mail marketing. However, messaging to mobile devices brings a host of new technical and ethical issues. The main form of messaging to mobile phones is now SMS text messaging, but with the advent of RIM Blackberry devices, phones are being used more and more for viewing and responding to e-mails.

Since the mobile phone is arguably a more personal device than the fixed PC, companies can be even more unpopular if they are perceived to have delivered spam. There is also the constraint of the limited space for communicating by SMS (restricted to 164 characters). How do you explain your offer and proposition in this space without recourse to a landing page for the direct response? Although these current limitations are significant, they will be

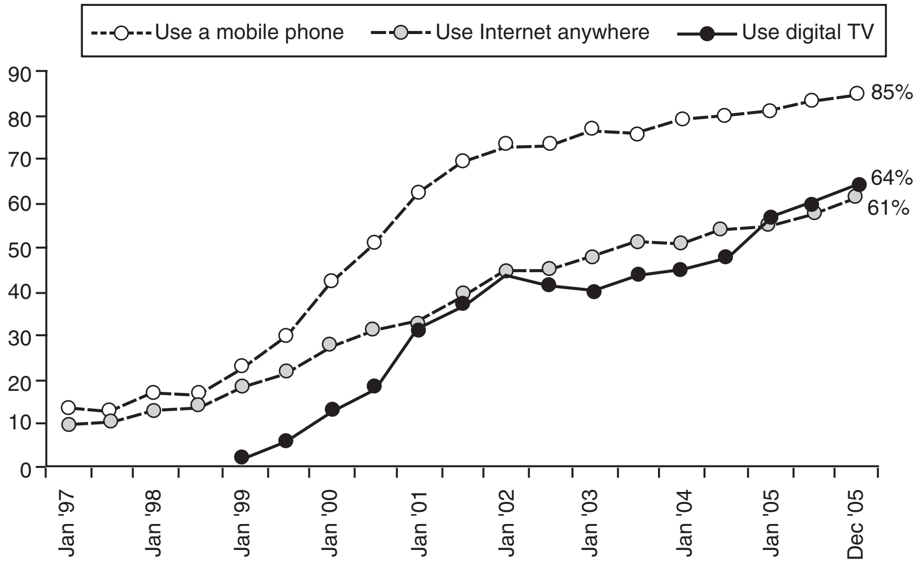

Figure 8.4 UK rate of adoption of different new media

swept away in the future by the advent of new-generation phones which use the wireless Internet to access e-mails using conventional inboxes such as Outlook Express. Many users already access their e-mails on their mobile through Yahoo!, but the limited, largely text-based user interface offers limited potential for marketing. The new technologies, such as WAP, GPRS and 3G, have been much criticized for their disappointing speed and the cost of the licences, but the technology will be widely adopted, worldwide. It is only a matter of when.

So, what are the options for mobile messaging and what are the latest developments? We start with mobile or wireless marketing and concentrate on the marketing applications rather than the technology. If you want to check out the technology, there's a good summary on Wikipedia (http://en.wikipedia.org/wiki/Mobile_phone) of the standards from 0G to 4G.

Mobile (m-commerce) or wireless commerce

We seem to like mobiles in the UK, Europe and Asia. The UK figures speak for themselves:

- 83 per cent of adults use mobiles
- there is 101 per cent mobile penetration amongst UK adults (some have more than one handset)
- more than 15 million handsets are replaced per annum, which is about a third of all handsets; the average upgrade time is 18 months
- 84 million text messages were sent person to person every day in the UK in April 2005
- 133 million text messages were sent on New Year's Day 2005 versus 111 million the year before.

If those numbers aren't mind-boggling enough, since recording started in 1999 we have sent over 100 billion text messages in the UK. (source: IDM, 2005, and Mobile Data Association; see www.text.it for the latest figures and case studies.)

In fact, in the whole of Europe there are 460 million mobiles, according to Admap (2005), which is much higher than in the US, where only 55 per cent of adults have mobiles.

Characteristics of mobile marketing

When thinking through the opportunities for mobile marketing, we should remember the inherent characteristics of the medium in order to best exploit its strengths and weakness. Chaffey (2004) describes the characteristics this way:

- Fixed-location web access is not necessary; this is more convenient for the user, who is freed from the need to access content via the desktop. This makes access possible when commuting, for example.
- Location-based services are possible. Mobiles can be used to give geographically-based services – for example, an offer in a particular shopping centre. Future mobiles will have global positioning services integrated.
- There is instant access/convenience. The latest GPRS and 3G services are always on, avoiding the need for lengthy connection.
- Privacy. Mobiles are more private than desktop access, making them more suitable for social use or for certain activities such as an alert service for looking for a new job.
- Personalization. As with computer-based access, personal information and services can be requested by the user, although these sometimes need to be setup via PC access.
- Security. In the future, mobiles may become a form of wallet; however, thefts of mobiles make this a source of concern.

A further issue related to privacy is the legal constraints involved, and it is vital that mobile marketers understand and comply with the Privacy and Electronic Communications Regulation 2003, which mandates that consumers opt in to receive text messages and can readily opt out. Several mobile providers have fallen foul of this or related data protection laws; see www.informationcommissioner.gov.uk for further details.

Some consumers will see their mobile as a personal device where they don't wish to receive promotional messages, and in this case it may be best to get them to opt in to receive e-mails. Using mobile messaging for permission-based customer communications is still at an experimental stage – maybe where e-mail was three to five years ago. We can expect a lot more brands to start giving the choice of text message contact, although it can be argued that e-mail is far more powerful since you are not limited to 60 characters and there is better response mechanism, which is a link through to a web site. Picture messaging, the growth in WAP sites and 3G phones will reduce these limitations.

Some areas of mobile marketing have worked particularly well – hair and beauty salons find mobile messaging great for updating customers on offers and boosting capacity when the salons are less full. Using SMS messaging to remind business people about events has also proved cost effective. As we become more familiar with such services, and if the value is there, it is likely that the opposition to these services will decline.

We have to respect consumer privacy and security fears with our mobile marketing, but remember that there are many opportunities to use the mobile to communicate with customers when they are away from their fixed web devices.

We will see that mobile phones have a great variety of response mechanisms which can be integrated with other media. These are often based around short codes – easy to remember five-digit numbers combined with text that can be used by advertisers or broadcasters for a personalized response from the customer.

Applications of mobile marketing

From the statistics above, you may think that the only application of mobiles is texting. Far from it; here are 20 marketing applications of mobile marketing, starting with the text-based ones. These are a summary of the main mobile marketing applications produced by Helen Keegan of Beep Marketing (author of the IDM (2005) module on digital marketing). The applications use Helen's categories, with my examples added.

1. *Text and win*. This is a convenient way to manage a competition or prize draw and is surprisingly popular with consumers. Think of the recent on-pack promotions by Walkers to win a million iPods – there was a draw every five minutes. Admap (2005) reports that a Cadbury on-pack 'Txt'n'Win' campaign offering £1 million in prizes received more than five million messages – a response rate of 8 per cent – thanks partly to the novelty of this approach and the ongoing popularity of prize draws.
2. *Voting and participation TV*. Text voting for reality TV programmes such as *Big Brother* and *The X-Factor* are incredibly popular (see Table 8.1).
3. *Quizzes*. Quizzes work well on mobile phones, using either text messaging or a java application for a deeper level of interactivity than text alone (graphics and sound can be incorporated). The typical way to start a quiz is to text in a keyword to a shortcode and a question is sent to you by return. Mobile quizzes are a good way for brands to engage

Table 8.1 Examples of popularity of different text messaging votes (source: Mobile Data Association)

Rank	Programme	Total number of votes by text message
1	*Big Brother 5*	> 10 million
2	*I'm A Celebrity Get Me Out of Here 2004*	> 10 million
3	*The X-Factor*	5.4 million
4	*Big Brother 3*	5.3 million
5	*Big Brother 4*	3.1 million
6	*Fame Academy 2*	1.6 million
7	*Eurosong 2002*	700 000

consumers. In 2005, Birds Eye asked consumers for their preferences for a new food style and combined this with the chance to win in a prize draw.

4. Mobile content (pictures, ringtones, video). Thanks to the popularity of ringtones, the mobile content industry is already huge and has increased rapidly.

   According to Cellular News (2005), a recent Mintel report put the UK content market at $1 billion, with ringtones accounting for the largest share of downloads (33 per cent of volume sales), followed by games (26 per cent of the market). The remainder is made up of wallpapers/screensaves (13 per cent), gambling (9 per cent), music (8 per cent) and others (11 per cent), which includes news updates from football clubs, the Stock Exchange and other special groups. The volume of sales is expected to increase from 30 million downloads in 2002 to an estimated 760 million in 2005 – a massive 25-fold increase.

   According to IDM (2005), brands are now capitalizing on the popularity of mobile content and are using it as part of their marketing effort. A picture or ringtone can be a second- or third-tier prize in a free prize draw or other competition which doesn't involve physically sending out many prizes.

   Any service such as a ringtone delivered by WAP can be invoked from a text message. For example, *Parker's Car Guide* now prints ad text 'go parkers' to 89080 (a short code) for quick access to the Parker's WAP site, which provides car prices 'on-the-go' at £1 for 10 minutes.

   And I managed to review mobile content without talking about the Crazy Frog!

   The popularity of online content is partly down to the ease of payment. No credit card is required, and no complex authentication. Users of services are simply billed through their network provider for these services. This payment service has been used in novel ways – for example, during the 2004 tsunami over £1 million was raised through SMS donations.

5. *Games*. Mobile games are very popular, and are even spawning new converged hardware. You may have seen addicts playing on the Nokia N-Gage or a Gizmondo. Again, these games make good low-cost competition prizes or incentives to sign-up for permission-based text or e-mail marketing. Coca-Cola has signed a deal to produce Coca-Cola branded games which customers will buy rather than download for free.

6. *Applications*. These are various types of productivity software that run on higher-end mobile phones which run the Symbian operating system or Windows CE. They can be used in a business-to-business environment for inventory and order tracking, as well as time management.

7. *Customer Relationship Management (CRM)*. Through combining some of the techniques above, such as offering mobile content for incentives and text messaging for communications, mobiles can be a useful element in a wider CRM initiative. It can help build relationships with consumers who don't have ready access to e-mail, or who simply find mobiles more convenient. The cost per message makes mobile CRM quite effective too, varying from 3p to 10p per message, according to volume.

8. *Interactive Voice Response (IVR)*. IVR is best (or rather worst) known as the system for connecting your call to the right department in large organizations, but it can also be used to pay for mobile content and for premium rate services in response to TV ad campaigns.

9. *Multi-media messaging (MMS) in/out*. This technique is increasing in potential as it becomes more readily available on handsets. However, it is limited by the cost and technical limitations of handsets. MMS can be pushed to the phone at higher costs than simple text messages (several times higher), or there is the cheaper option of 'virtual MMS' or WAP push. Here, the message is downloaded to the phone. Most marketers stick with text because it is cheaper and doesn't suffer these compatibility problems.

10. *Direct ad-response/Red Button Mobile*. Red Button Mobile describes direct-response campaigns using the mobile phone as opposed to using the red button on interactive television (or, potentially, outdoor or print advertising, unlike true red-button advertising). The mobile 'red button' is based on a shortcode available optionally coupled with different relevant keywords, dependent on the response mechanics. Options include:

    - text to screen – with TV, comments texted in can be automatically populated on screen as used by reality TV programmes (text to screen)
    - text to e-mail – where you text in your e-mail address to a short code and an automatic HTML e-mail is generated to the respondent
    - text to post – this works in a similar way, where you text your address or postcode and street number
    - text to WAP – here, respondents are directed to an advertiser's WAP site through a link where they can access content or opt in
    - text to mobile content – content such as a ringtone or a coupon is received through texting a shortcode.

    As an example of the potential effectiveness of these campaigns, Axa PPP ran a direct-response campaign involving press advertising for their personal health insurance provider. Customers were asked to respond to the advertisement either by freephone (0800 number) or via text message; 50 per cent of all the replies came via text message and all texts routed direct to the call centre to manage outbound calls.

11. *Barcodes*. Barcodes can be sent to a mobile phone and then redeemed in-store using the usual Epos systems. For example, Ann Summers uses this technique if you text in response to a print or other advertisement (so I am told!). There are practical issues with this owing to the large number of different handset displays on which the bar code has to be displayed. A new take on bar codes is 'camera codes', where a consumer takes a picture of the barcode from a TV screen, poster, newspaper, magazine or website, or anywhere really. This then initiates the response mechanism or can be used for couponing.

12. *Location-based services (LBS)*. This technique has been prominent recently, with companies offering services that allow children's whereabouts to be tracked via their phones. With ChildLocate, parents pay a monthly fee of £9.99 to have access to the service. The monthly fee includes 10 free location requests and 10 free text messages. Additional

location requests are charged at 30p and text messages at 10p. Trials have also been run in shopping centres, where shoppers can opt in to receive promotions, but this is generally seen as an idea implemented before its time. 'Find me' services are available, which are useful for evenings out, and the mobile version of Google can also help with this.

13. *WAP portal*. WAP sites are the mobile versions of media sites, such as the BBC or Channel 4 or the network owner. WAP e-mail is also popular on some smartphone or PDA devices – check your e-mail renders clearly on these devices in text mode.

14. *Java portal*. This is a different form of portal, where you do not have to visit the portal but instead content is downloaded in line with your preferences. Avant Go! uses this technique to download content while a smartphone is being synchronized with a PC.

15. *Mobile search*. All the main search providers have mobile (WAP)-specific versions of their search engines. These are now becoming more sophisticated. Google Mobile search (www.google.co.uk/mobile) offers Local search to find a local business, and will then display a map (Google Maps is integrated) or phone number with the option of click-to-call on the appropriate handset. Google Local uses listings from Yell.com.

16. *Mobile music*. Beyond ringtones, many handsets are now designed to play and store MP3 music files and potentially rival the iPod – although we now have an iPod mobile version. As access speeds increase, tunes may be offered in promotions.

17. *Podcasting*. Podcasting involves streamed delivery of a radio programme, tune, speech or video. Podcasts can be accessed on any device with the appropriate MP3-playing capabilities (see http://www.voxmedia.org/wiki/How_to_Podcast).

18. *Blogging and RSS*. Blogs are proving incredibly popular with those in the know. Technorati (www.technorati.com) lists around 20 million blogs (it is estimated that around 3 per cent of American are bloggers, while more than 60 per cent read blogs). RSS feeds of blogs (see http://www.wnim.com/archive/issue2203/new_media_innovation.htm) can also be accessed by mobile. While this format works best on conventional fixed web access, mobile blogging is used by those on the move. RSS and blogging are described in more detail at the end of this chapter.

19. *Moblogging*. Moblogging (or blogging from your mobile phone) is possible and, although it can be text-based, makes best use of the potential of the device when images or video clips are submitted by MMS or WAP. We now have citizen journalists who report breaking news before the main networks. Sony Ericsson has used the technique of posting images to a blog to promote its K300i phone, by encouraging users to upload their images to http://www.shameacademy.com.

20. *Bluetooth/infra red*. These techniques enable a message to be sent from one electronic device to another. From a marketing application viewpoint, we are only just starting to see this technique used (many phones don't have Bluetooth). While individuals can exchange a business card or use their phone as a modem which links by Bluetooth to their mobile, a much more exciting application is Bluecasting. This technique was used with the launch of the latest Coldplay album, where a London-based campaign involved 13 000 fans downloading free pre-release video clips, never before seen interviews,

audio samples and exclusive images onto their mobiles via Bluetooth from Transvision screens at mainline train stations.

In this campaign, 87 000 unique handsets were ‘discovered’ and 13 000 people opted-in to receive the material – a response rate of 15 per cent. The busiest day was Saturday 4 June – two days before the official album launch date – when over 8000 handsets were discovered and over 1100 users opted in to receive a video file. The Bluecast systems can deliver time-sensitive content – so, for example, in the morning the users would get an audio clip of the tracks *Fix You* and be prompted to tune in to Radio One, and in the afternoon the clip would be the same but users would be prompted to watch Jonathan Ross on BBC1.

And yes, in case you’re wondering, the first cases of Bluejacking other phones, Bluetooth viruses and Bluespamming have already been reported.

REALLY SIMPLE SYNDICATION

The last technology we will review is arguably the most exciting. I believe that in the long term it will both complement and rival e-mail as a strategic marketing communications medium.

From a technology view point, Really Simple Syndication (RSS), also sometimes known as Rich Site Summary, is an Internet standard for publishing and exchanging content using XML. From a practical viewpoint, it enables two things. The first is that content can be syndicated or published on one site that originates on another site. Secondly, and of much greater interest to the e-mail marketer, it is a relatively new method of distributing messages to subscribers.

At the time of writing, most consumers and few business people have heard of RSS – it is mainly used by journalists and analysts as a convenient way of keeping up to date with press releases. Initially the RSS messages were received by specialist software that could be downloaded for free, such as RSS Reader (www.rssreader.com), or sites that receive feeds, such as Bloglines (www.bloglines.com). These RSS readers, or aggregators, poll for RSS at a defined interval, often once an hour.

RSS will not become widespread until it is incorporated into standard software, but this will happen. In 2006 you can receive RSS feeds within your web browser, and once they are included as a different type of inbox within e-mail packages, I believe they will be much more widely used. Currently, though, the proposition of RSS against e-mail isn’t strong enough for most audiences, although it is superior for some audiences such as journalists and technology followers. I also think improvements to the RSS readers to incorporate features similar to e-mail packages, such as rules and keyword-based filters, will help to manage the volume of RSS.

RSS has been embraced by major publishers such as the BBC, and if you visit the BBC web site, you can see its potential. It enables you to subscribe to very specific content that interests you, and then provides you with an alert when a new story is published. For example, I subscribe to the e-commerce news channel and that for Arsenal, my football team. In this arrangement subscription does not require opt-in, it just requires a request of the feed.

RSS is therefore potentially a threat to the permission marketing model, since there is no data exchange and it is easy for subscribers to switch on and off.

RSS will become much more widely adopted when it extends beyond specialist readers to the still ubiquitous Internet Explorer and Outlook products. Going forward, e-mail marketers need to manage the risk of reduced use of permission-based e-mail as customers realize the benefits of RSS, including:

- more granular control of communications (e.g. customers can choose content updates from any channel on the BBC site, such as the e-commerce section (see the BBC web site for an explanation of the RSS consumer proposition)
- that it can be switched on and off without registration, which reduces the control of marketers – someone could subscribe to holiday offers within a two-week period from a travel web site, for instance
- little or no spam, since messages are pulled to the reader from the server (this is currently the case, although ads may be placed within a feed).

There are certainly disadvantages to RSS from the consumer viewpoint. It requires a separate inbox or reader to set up and monitor, and this has deterred many. It also only suits certain types of information, published as single alerts, so it is mainly used for short stories and press releases. It has not traditionally been used in a newsletter-type format with an edited collection of stories, but this is possible within the specification.

RSS is a threat to e-mail marketers because typically users profile and qualify themselves before opting in to e-mail. With RSS this permission marketing isn't necessary, since it is a pull service where the user retrieves information from the web site hosting the RSS feed. The user just subscribes to the feed without the need to share any information with the organization. This has been the typical model to date, but Silverpop has recently launched RSS Direct, which uses a more familiar e-mail permission marketing model where the user provides information before signing up to feeds. I'm sure many e-mail marketing service providers will move to offer this service, and indeed the data-capture technology looks straightforward – involving simply placing a data-capture form with which to configure the feeds – so could also be implemented in-house.

It will be interesting how this plays out over the next couple of years. Will marketers provide free access to RSS to maximize volume of subscribers, but be limited by their capability to profile and target customers? Alternatively, they may use the permission-based opt-in RSS model, which will have lower volume but improved profiling and targeting.

RSS certainly presents opportunities for new types of communications. As the BBC web site shows, subscribers can access much more specific, timely information, and from the content-providers' point of view, all they have to do is publish it on the site and subscribers will be notified. Marketers will have to think how the page layout of the template can be used to achieve wider objectives, such as generating awareness, interaction and response (for example, sign-up to e-mail subscription). In some sectors RSS has potential – updating about new holiday offers (perhaps you will just switch it on for a two-week period, for example, to just show holiday deals in Cuba), books from a favourite author, or new gadgets from a favourite supplier.

In reality, I think more complex e-mail/RSS communications preferences will be offered to consumers. Perhaps certain types of high-value information will only be offered through e-mail. Time for some more testing …

REFERENCES

Admap (2005). How marketers can exploit new mobile services (by Dan Steinbeck). *Admap*, **Jul/Aug**, 41–43.

Cellular News (2005). UK Mobile Content Market Worth Over US$1 Billion. Article dated 22 September (available at http://www.cellular-news.com/story/14147.php).

Chaffey, D. (2004). *E-business and E-commerce Management*. FT-Prentice Hall.

IDM (2005). Course material on IDM Certificate in Digital Marketing – modules on mobile messaging and interactive TV and Radio. IDM.

Newmediazero (2002). E-mail marketing warning. *NewMediaAge*, **April**.

WEB LINKS

Mobile Marketing Association (www.text.it)
SPAMcop (www.spamcop.net)
SPAMAssassin (www.spamassassin.org)