

**Email Marketing: Challenges in Channel
Management**

Yajun Fang

Taeko Okano

Stanley Trepetin

Prabhakar Vaidyanathan

15.567 Introduction to e-Commerce

Final Project

A. Introduction

Firms must be careful while they conduct email marketing. Email marketing appears attractive because its costs are significantly lower compared to other forms of advertising.¹ Thus email marketing appears to be an inexpensive way to increase brand awareness and sales.² Unfortunately, these advantages have led to an overuse of email marketing,³ focusing increasing public attention on its opposite and detractor, that is, spam. Consumers, ISP's,⁴ even legislators are worried that unsolicited commercial email (UCE) is undermining email as a communication channel. UCE fills consumer email boxes and forces ISPs to upgrade their facilities to handle increased email traffic. Laws have even been passed to mitigate this problem.⁵ Thus firms wishing to advertise using email face a dilemma: how should they leverage this productive sales channel while minimizing the risk of being associated with "spam"? This study suggests that disciplined management of the email-marketing channel will ensure its success for the firm.

B. Focus

Firms must handle the legal, ISP, and consumer concerns to successfully manage the email marketing campaign. Advertising does not operate within a vacuum but within the legal, channel, and recipient contexts in which it is embedded. For example, for US direct mail, the requirements of US laws, the United States Postal Service, and US citizens must be understood. In the case of email marketing, these become UCE laws, ISP rules, and consumer preferences which must be understood. These must be followed if the advertising campaign is to succeed.

B.1. Scope

This paper focuses on a retail⁶ firm based in the United States, conducting email marketing on the

¹ Diane Anderson, "E-Mail or Me-Mail?" March 6, 2000,

<http://www.thestandard.com/article/display/0.1151.12422.00.html> (cited: November 15, 2000)

² Joe Dysart "E-mail marketing grows up." *Security Distributing & Marketing*; Newton; Feb 2000 P145-149

³ Barnes and Nobles promised to stop sending unsolicited emails to consumers in 1997 but did so again in 1998, due to competitive pressures, as it was an effective promotional tool.

<http://people.delphi.com/lfarrantello/nospam/spammers.html#Amazon> (cited: November 3, 2000)

⁴ In this paper, Internet Service Provider will include wire-line and wireless Internet providers such as AOL.

⁵ See, for example, www.spamlaws.com, citing laws in the United States and Europe. Cited: October 13, 2000

⁶ In this study a retailer is the manufacturer, distributor, and seller of goods, such as Gap, Amazon.com, and

Internet and mobile phone platforms in the US and Europe (EU). By focusing on a specific part of the email marketing space, the results will be generalizable. The selected parameters were specifically selected to be generalizable.

Focusing on the US retailer is a credible representation of all firms advertising online since retailers are the largest advertisers. For example, in 1998 and through the third quarter of 1999, consumer-brand related advertising was the most advertised category online.⁷ US-based retailers have to be some of the biggest spenders as it is a new channel they are extensively exploring.⁸ Thus US retailers are representative of all online firms.

Focusing on Internet and mobile phone platforms represents all current and future email marketing platforms. The Internet (such as desktop) email platform is the largest current email marketing platform⁹ while Mobile phone platforms represent the future wireless market. For example, by 2002, 70% of US consumers will have wireless phones.¹⁰ Therefore, the current and future email *trends* are representative of the email space as a whole.

The US and Europe represents the largest space of email marketing recipients since the largest percent of email users reside in these two regions. In 1998, the US had 30.5 million Internet hosts while the EU had approximately 5 million, the largest and second largest number of hosts, respectively.¹¹ Hosting includes services to route TCP/IP packets to their destination but also must represent the local expertise and interest in Internet usage.¹² Otherwise, hosts would be placed in close proximity to one another, representing a disinterest in expanding geographically. The distant placing of hosts suggests people are interested in Internet capability. Therefore, the amount of interest in Internet services should be the largest in US and EU. Since email is basic among such services, US and EU email interest should represent worldwide email interest.

We also assume that retailers want to behave ethically. By legitimately satisfying consumer demand

Gateway.

⁷ Internet Advertising Bureau <http://www.iab.net/> Cited: November 3, 2000

⁸ Personal knowledge.

⁹ Personal knowledge.

¹⁰ Jade Boyd "The Web Goes Wireless -- Popular site operators set their sights on mobile users": *Internetweek*; Sep 11, 2000, P27

¹¹ ITU: International Telecommunication Union : Internet indicators http://www.itu.int/ti/industryoverview/at_glance/Internet98.pdf Cited : November 31, 2000

¹² personal knowledge.

they can achieve the desired ROI. That is, ethical business often leads to long-term financial success.¹³

C. Law

The paper will focus on Federal US and EU laws since they represent the trend in legal infrastructure in both regions. By doing so the legal ramifications of email marketing in both regions can be understood. In the US and the EU there are almost 20 anti-spam Federal laws (mostly pending but some have already passed)¹⁴ and dozens more at the State level.¹⁵ We will focus only on Federal anti-spam laws. This is done because: 1) the majority of the “states” in the US and the EU do not have strict anti-spam regulations,¹⁶ thus the Federal laws should become the laws for the region and the laws that firms should follow; 2) the state and Federal laws in US and EU are similar enough in content, therefore, discussing the Federal law will subsume the discussion of the State laws.. Also, given the intensity of the current debate on and political support against spam, pending anti-spam legislation probably will pass. Therefore, near term legislation will also be highlighted to understand firm impact.

C.1. United States Law

Currently, there is no specific "anti-spam" federal law. There have been attempts to use existing anti-junk fax law (US Code 47.5.II) against UCE. This law restricts the ability of advertisers to send unsolicited messages to FAX machines on the grounds that the recipient bears the costs of receiving them.¹⁷ There is insufficient legal precedent for this law in terms of historical cases, therefore its potential impact on a firm is uncertain. However, biased content emails have been prosecuted in the past.¹⁸ For example, the FTC has prosecuted email chain letters and pyramid schemes.¹⁹

¹³ Larry R Smeltzer, Marianne M Jennings “Why an international code of business ethics would be good for business” *Journal of Business Ethics*, Jan 1998 P57-66

¹⁴ Spam Laws www.spamlaws.com Cited: October 13, 2000

¹⁵ A State will mean a US State such as Washington State or an EU country such as France. Also, for US State laws, see *Privacy and American Business*, Sep.1999

¹⁶ So far, in EU, Austria, Finland, Germany, and Italy, or the minorities of the fifteen EU Member Countries, have strict anti-spam laws (although others are considering them). In the US, 18 of the 50 States have enacted anti-spam legislation since 1997, again so far a minority.

¹⁷ Broadcast Fax and Junk Email Illegal <http://www.markwelch.com/faxlaw.htm>, Cited: November 14, 2000

¹⁸ JunkMail: Junk Email lawsuits Online <http://www.junkemailmarketingail.org/lawsuits/> cited: October 20, 2000

¹⁹ FTC: Federal Trade Commission, Press Conference on “Spam,” July 14, 1998,

In terms of near future legislation, the Unsolicited Electronic Mail Act of 2000 (H.R. 3113) should probably pass soon. It has reached the stage of Congressional House of Representatives approval, further than any other bills. Given existing anti-spam sentiment it should pass soon.²⁰ HR 3113 states:²¹

1. UCE is allowed until the recipient requests to opt-out, at which point subsequent UCE is unlawful.
2. UCE must be identified as such (for example, in the SUBJECT line) and must offer opt-out instructions.
3. UCE sender must adhere to ISP UCE policies, whatever they may be.

C.2. EU law

The EU has been more active in creating anti-UCE laws. The key piece of legislation governing UCE is the EU Data Protection Directive 95/46/EC.²² The directive includes the following:

1. Purpose limitation: data must be collected and possessed for specified, legitimate purposes.
2. Data Transfers: without consent, a consumer's personal data cannot be transferred to third parties unrelated to the current transaction.
3. Firm Organization: Organizations processing data must appoint a "data controller" responsible for all data processing, who must register with government authorities.
4. Individual Redress: An individual must have the right to:
 - a. Access information about oneself.
 - b. Correct or block inaccuracies.
 - c. Object to use of information.

The Directive was amended in 1999 requiring consumers to join a national "opt-out" list if they wished to stop receiving UCE.²³ Thus the Directive has become an opt-out directive, i.e.: it makes it legal for a firm to send UCE in the absence of explicit consumer opt-in. The directive also suggests that the following practices will be soon required:

1. The UCE sender his message must be clearly identified.

<http://www.ftc.gov/opa/1998/9807/jbspam.713.htm>: October 9, 2000

²⁰ Spam Laws www.spamlaws.com Cited: October 13, 2000

²¹ Spam Laws www.spamlaws.com Cited: October 13, 2000

²² Rotenberg, Marc. *The Privacy Law Sourcebook 2000*, p287-p288.

²³ Felicity Ussher "Euro ISPs slam EU e-mail law" May 10, 1999

<http://www.silicon.com/public/door?REQUNIQ=926324049&6004REQEVENT=&REQINT1=30098&REQSTR1=newsnow> Cited: November 10, 2000

2. UCE should not result in additional communication costs for the recipient.

C.3. Impact of US law

To follow legal guidelines in the US, the retailer must:

1. Ensure that email advertising is free from bias (for example, deceptive advertising).
2. Ensure that email advertising is labeled appropriately, and provide opt-out instructions.
3. Honor opt-out requests after consumer initiates an opt-out request, do not attempt further email contact. One suggestion is to use opt-out filtering technologies, such as the one used by Apex Global Internet Services Inc, an Internet backbone provider.²⁴
4. Adhere to anti-spam policies of ISP (discussed in section D).

C.4. Impacts of EU law

Similarly, when conducting an email campaign in the EU, a retailer must:

1. Make sure its privacy policy is specified and fully followed.
2. Employ a data controller on site to liaison with government representatives. The retailer should consider employing a Chief Privacy Officer (CPO) for this task. A CPO's function is to allay consumer privacy concerns. Given that email marketing might involve such concerns, the CPO should handle email marketing issues as well.²⁵ Internet firms like Doubleclick and Excite@Home and Fortune 500 firms like AT&T and Microsoft have or recently have appointed CPO's.²⁶
3. Make sure that it does not transfer data to unrelated third parties without customer permission.
4. Provide access, correction, and blocking capabilities to consumers on information about themselves. This will not be trivial because the law is unclear on what is meant by information "about oneself?" If it includes non-personally identifying data such as clickstream data (e.g. Websites visited, search engine query terms, click-through responses to advertisements, etc.), then this could be technically challenging. Such data is tied to a computer or browser, which may be used by several individuals in the same location, making identification difficult. It also does not

²⁴ Randy Barrett "Opt-Out Spam Filter Hits Technical Glitches" June 23, 1997
<http://www.zdnet.com/intweek/print/970630/inwk0019.html>. Cited: November 9, 2000

It is unclear if such technologies exist today given that the original filter vendor appears to no longer exist.

²⁵ Personal knowledge

²⁶ Daniel Weitzner, Talk on Privacy and Pervasive Computing, November 20, 2000, Massachusetts Institute of Technology; *Washington Telecom Newswire*, June 20, 2000; Ann Harrison, "Microsoft backs P3P net privacy standard," *Infoworld Daily News*, April 12, 2000.

define a scope and security for access – for example, the fact that a user defaulted on a loan should not be able to be altered by a user.²⁷

However, email marketing uses non-sensitive data about an individual like his email address and interests and preferences, therefore creating a robust information data management system should not be overly challenging. For example, the Children’s Online Privacy Protection Act in the US requires similarly rigorous features to be implemented on behalf of children. In order to comply with the COPPA regulation, firms have had to invest between \$25,000 and \$150,000 in systems to ensure that their websites interact with kids only after satisfying requirements such as, getting parental consent, posting proper warnings, etc.²⁸ Therefore, retailers might have smaller costs given the less sensitive nature of the data.

5. Check national opt-out databases before conducting email marketing. Currently there may be several national opt-out list in EU countries. The challenge is in checking all the lists before proceeding with the campaign.
6. Clearly and truthfully identify UCE sender and her message.
7. Make sure that the recipient does not incur extra costs to receive UCE. This requirement will make it very hard to send UCE since costs to a user arise from two aspects email characteristics:
 - a. The Internet service cost (for example, the monthly Internet base rate). Costs to an ISP may increase because ISPs incur costs to add more capacity to move more UCE traffic²⁹. The ISP in turn may transfer these costs to consumers through a price increase.
 - b. Per minute charges to download a UCE from a server (even if it is to be deleted later because it is spam).

Ideally, such users should be identified and targeted only if they have “opted-in” to receive such emails.

C.5. Multi-country solicitations

Firms also need to be aware of cross-country email interactions. Depending on the complexity of the advertising relationships, the retailer should follow either the Safe Harbor Principles or the full EU law for compliance. If the retailer can identify customers as EU citizens currently on EU soil,

²⁷ Jason Catlett, President, Junkbusters Corporation, presentation during U.S. Chamber of Commerce conference on Online Privacy, July 20, 2000.

²⁸ Carolyn Duffy Marsan, “Net privacy law costs a bundle,” *Network World*, May 15, 2000, p.117.

²⁹ Personal knowledge.

then it can chose to follow the Safe Harbor Principles. This US-EU agreement protects EU citizens by requiring US firms to adhere to a set of principles similar to the EU Data Directive when handling the personal data of EU citizens. However, the Safe Harbor Principles are simpler and less expensive to carry out than the EU Data Directive.³⁰ For example, the Principles do not require a government liaison. The Principles require a US firm to provide:

1. Notice of their information practices.
2. Choice as to whether and how personal information may be disclosed to third parties.
3. Transferability of personal data to third parties consistent with the notice and user choice.
4. Security for personal data, at its creation, maintenance, use and transmission.
5. Access to individuals to the information that a firm holds about them with regard to email marketing and the ability to correct, amend, or delete inaccurate information.
6. Enforcement mechanisms to assure compliance with the foregoing principles, and recourse for injury.

Yet, the difficulty in identifying EU citizens and the complexity of possible advertising relationships suggests that following the EU Data Directive is the strongest way to mitigate risk. Identification of citizenship requires analysis. Just because a person is located in EU does not mean she is a EU citizen. She might be a student, a traveler, etc. The retailer would have to understand this. Otherwise, it would feel the necessity to upgrade its systems completely to provide disparate data protections to its users. Furthermore, real life e-commerce can generate complex relationships with overlapping jurisdictional boundaries, leading to uncertain legal standing. For example, a US retailer could solicit a European citizen on US soil using a website which is powered by European servers in Europe! What level of data protection must a firm provide in such a circumstances? Given the difficulty of authentication, and the fact that no international law currently exists for complex cross-jurisdictional boundaries, the best choice would be for the retailer to follow the stronger EU law and reduce business risk.³¹ Otherwise, litigation costs and poor brand image may result.

D. ISP concerns and Impacts

ISP's are also concerned about UCE. They are adopting anti-spam policies to prevent abuse of their

³⁰ Taken from School of Law, Santa Clara University. *Santa Clara Computer and High Technology Law Journal*. May, 2000

³¹ Professor Chuck Caldart, MIT interview with authors, November 18,2000.

infrastructure. A Gartner Group study shows that the overall cost of spam to an ISP is \$7.7 million per million users (most of which comes from losing customers who get tired of spam). Consequently, ISP industry groups have come together to resolve the problem. They have promulgated the “Best Current Practices” (BCP) standards³² to restrain UCE senders by restricting their email capabilities.

BCP has a number of suggestions which ISP’s must follow. First, there are strict rules as to how ISPs can interact with companies associated with UCE. One requirement is that ISP’s will not relay email for “unauthorized parties.” “Unauthorized Parties” have not been specifically defined, but a guideline that has been to use the so-called “black hole / filter” lists. These lists comprise of companies that have been associated with spam by various independent observers.³³ People such as Paul Vixies,³⁴ use sophisticated UCE TCP/IP tracking tools to find UCE senders. If transmission is repetitive or meets other criteria, Paul places the company on the “black hole” list with the intent to control the spam problem. Since ISPs are also interested in such control, they have started adopting Paul’s and other similar lists for their own purposes. The result is that when firms get on the lists, ISP’s assume that they are spammers and block their emails. For example, America Online used Paul’s list to block Harris Interactive’s (HI) – a survey company’s -- access to its users, presuming HI would spam its (and AOL’s!) users again.³⁵

Another requirement is that ISPs disclose information about resolving spam problems. BCP specifically requires disseminating information on actions taken to resolve specific abuses. The audience for such dissemination is unclear, but given that ISP’s are trying to stop the spam problem, it’s possible they would make the case public. Public disclosure would put great pressure on the firm to change its UCE practices since this results in poor brand publicity. It may also encourage future lawsuits.

³² LINX Best Current Practice for combating Unsolicited Bulk Email May 18, 1999 <http://www.linx.org/noncore/bcp/ube-bcp.html>. Note that although we didn’t see wireless phone best practices standards in researching this paper, a representative from a major wireless phone manufacturer indicated its company’s fears concerning UCE. UCE can be a nuisance, such that consumers give up their phones. Thus, BCP should be followed by all ISPs, not just wire-line. (Interview with authors, November 20, 2000).

³³ Jesse Berst “New ways to stop spam”: February 13, 1998 http://www.zdnet.com/anchordesk/story/story_1693.html Cited: November 13, 2000

³⁴ Vixie’s anti-spam campaign <http://www.vix.com> Cited: November 20, 2000

³⁵ “Harris Interactive Fails In Effort to Receive A Restraining Order,” *Wall Street Journal*, Aug 9, 2000, p.C.6.

The retailer must adapt to these BCP requirements. First, retailers need to find out about the black hole lists and should monitor all of them to make sure they are not on them. Although these lists are uncoordinated, the retailer must make sure it is not on any of them for its own sake. If a retailer gets on such lists -- either by mistake or because it sent emails that were beyond the bounds of permissible emails -- it should quickly correct the situation. A retailer can apologize to the ISP or understand why they were put on the list in the first place, to avoid such instances in the future.³⁶

BCP standards also have technical requirements, which must be followed. Key requirements include that all email generated within an ISP's network should be:

1. Traceable to its source.
2. Attributable to a particular customer or system.

Therefore, retailers must ensure their email marketing systems send only readily traceable emails.

E. Consumer concerns

Finally, consumers must be satisfied with the emails for the campaign to succeed, otherwise sales will not materialize³⁷. By involving consumers in the advertising process the retailer's can ensure their support.

E.1. Don't target without consent

Consumers are interested in creating products offerings for themselves as they can create products of most personal value. Therefore when creating email marketing campaigns, retailers should involve consumers in the process. Consumer permission should be asked to ensure that they wish to be involved, otherwise the effort might fail. Consider campaigns that do not involve similar interaction, such as "online profiling." In this technique, websites anonymously track customer "interests" via clickstream interactions, including linking such data with personal or psychographic (e.g. demographic, purchase-tracking, etc) data offline.³⁸ The intent is to understand a consumer's interests – without asking them directly in order to tailor advertisement offerings to them.

³⁶ Randy Barrett "Crusader Conducts Spam War" May 19, 1997

<http://www.zdnet.com/intweek/print/970519/inwk0055.html> Cited: November 22, 2000

³⁷ "Marketing without consent: Consumer choice and costs, privacy, and public policy" Spring 2000 *Journal of Public Policy & Marketing* Cited: November 14, 2000

³⁸ FTC: Federal Trade Commission - Such as offline purchases, voting records, etc pp.4-5 www.ftc.gov Cited: October 9, 2000

Online-profiling is easier, while seeking explicit customer consent is difficult because statistics show that only 10% of individuals will opt-in when request to. This could be because they may not be interested, or may not know how to opt-in etc.³⁹ Online profiling however is not as effective as the consent-based approach. For example, consider the fact that banner advertising, which uses a similar methodology has been poor at generating sales.⁴⁰ This is because tracking mechanisms have mismatched consumer interests with the advertising served. Although some sources claim banner ads are effective⁴¹ other online advertising formats are proving even more so.

E.2. Associate with permitted communication flow

A more proactive method is to serve advertisements using existing and permitted communication flows. Firms regularly send newsletters, shipping confirmation emails, monthly billing emails, etc. to their customers for standard business communications. By including advertising in such channels, the channels legitimize the campaign. It becomes similar to advertising in other media (e.g. television), where consumers adapt to advertising because it is part of the service that is provided.

E.3. Opt-in marketing

Finally, the most consumer-involved approach is opt-in marketing. It has been rising in popularity.⁴² In opt-in marketing, a firm seeks customers' consent before information is forwarded to them. Opt-in marketing offers several advantages since consumers themselves select the material they wish to receive:

1. Consumers, having opted-in, will be interested in the email campaign, raising brand awareness.
2. Consumers will provide more accurate personal information, letting marketers tailor the most appropriate product and service offerings.
3. This may generate repeat sales from customers because they feel their needs are being addressed.

³⁹ Personal knowledge.

⁴⁰ Terry Sweeney, "WEB ADVERTISING -- Online Advertisers: Money To Burn -- Click- through rates on online ads are declining, but true believers say there's no place like the Web to build the brand," *Internetweek*, Oct 9, 2000

⁴¹ Kevin O'connor, talk in "ecommerce" class at MIT, November 29, 2000.

⁴² Dian Anderson "E-Mail or Me-Mail?" March 6, 2000

<http://www.thestandard.com/article/display/0,1151,12422,00.html> Cited: October 30, 2000

For example, in the wireless phone arena, a theatre can form a partnership with a news and entertainment website like CNN wireless. When consumers choose CNN wireless as a part of the service offering – by selecting them in a wireless preferences platform such as WinBox.com⁴³ -- they can be asked if they are interested in receiving location-based discount theatre tickets. Then theatres can send them an advertising a few minutes before showtime if the consumers are nearby and the theaters have excess capacity. Consumers will probably purchase the tickets because they indicated their interest in doing so.

Although the benefits sound good, one question that is puzzling is as to how the firm should go about getting its potential customers to opt-in in the first place? How should the firm make first contact? The problem is that for customers to “opt-in” they must know how and where to opt-in, and since the firm has not had a prior relationship with them, this will be unclear to them. We see that the opt-out approach is useful to reach an individual with whom there had been no prior contact. On the other hand, the opt-in approach is better for all subsequent contact because the consumer will be interested in the advertising. Therefore we can combine an opt-out and opt-in approach as one possible approach. We can call this, a *one-time opt-out and subsequent opt-in policy*. In this approach a retailer sends a single UCE to consumers, in an attempt to get them to opt-in. The email will contain clear instructions how to opt-in. If consumers do not respond, the retailer should assume they are not interested and attempt no further contact. But if the consumers opt-in, the retailer can proceed with a customized campaign, like before, with all its contingent benefits. Note that such a process should only be attempted in the US as it will be illegal in the EU (burdening users with UCE costs). Of course, the retailer can also use regular advertising mediums like television or radio to promote user traffic to its opt-in website.

A less intrusive (but more costly) method is to acquire opt-in “lists” from brokers or “loyalty” list programs. Providers – such as YesMail.com (a broker)⁴⁴ and MyPoints.com (a loyalty program)⁴⁵ -- collect opt-in data from websites, surveys, and other customer relationship instruments for trading with other firms. The retailer can acquire such lists in order to target and provide the desired services to list participants.

⁴³ WinBox.com-Mobile Messaging <http://www.winbox.com/winbox.Page> Cited: November 30, 2000

⁴⁴ Yesmail.com www.yesmail.com Cited: November 1, 2000

⁴⁵ My Points.com-reward yourself <http://www.mypoints.com/?MCK=12ac01b53a289adc> Cited: November 15, 2000

In any case, opt-in marketing will lead to a smaller customer base. The opt-in campaign targets consumers who *want* information, not the consumers who might want it but could not explicitly opt-in for a variety of reasons. Since a smaller population is exposed to advertising, sales volume may be less. On the other hand, given the higher sales conversion rates of a *product-interested* customer base, opt-in email marketing may still compensate for a smaller advertisement base.

F. Special Considerations for Wireless

When doing email marketing through wireless phones, there are other issues.

F.1. Platform

The wireless platform has several limitations. The display screens on current mobile phones is small, minimizing text placement and visibility. For example, AT&T Digital PCS users can receive a total of only 150 characters in the message text, which includes the name in the FROM: field and a topic in the SUBJECT: field.⁴⁶ Also, consumers often pay for receiving emails, unsolicited or otherwise; and these costs are not trivial. For example, starting October 31, 2000, One2One wireless phone service the U.K.⁴⁷ requires its users to pay a 10 pence charge for each text message received, and also for a *notification* that a message was received. Users may also pay roaming charges when they move out of their designated cellular area.⁴⁸ Finally, when specifying opt-in, the time *when* one wishes to receive advertising cannot be specified. On many existing wireless preference platforms—such as MyAlert.com (for GSM mobile phones)⁴⁹ – users cannot specify the day of the week, or the time of the day when they would prefer advertising to be sent.

F.1. Retailer Response:

These limitations require several retailer actions.

1. The retailer should seek opt-in for all wireless email advertising to avoid users from incurring

⁴⁶ AT&T Wireless Service http://www.mobile.att.net/mc/personal/pager_show.cgi Cited: November 27, 2000

⁴⁷ one2one <http://www.one2one.com> Cited: November 29, 2000

⁴⁸ Personal knowledge.

⁴⁹ MyAlert.com- all in your mobile

http://www.myalert.com/MyAlert/pregenerated_homepage/frmGuest_English.html Cited: November 25, 2000

UCE phone charges (which is also illegal in the EU).

2. The retailer must shrink the advertising to fit the phone display. The retailer can produce small emails for both its Internet and wireless campaigns, avoiding the expenses to shrink the ads for the phone (in the form of software upgrades, content redesign etc). However, the retailer may need to maintain the larger Internet ads if they are useful to generate more sales. The decision will depend on the specific case at hand.

3. The retailer should partner with list brokers (or use its own legitimate communication channels) to get time sensitive wireless opt-in information from consumers. Consumers should be asked about their time preference to receive emails and the resulting responses should be used to time the advertising campaign.

G. Implementation considerations

G.1. Partner interactions

To improve email marketing, the retailer should partner with other email marketers. Combining products, systems, customer lists and expertise can lead to synergistic campaigns. On the other hand, the retailer must be careful about the marketing policies of the partner and the privacy concerns that linking data together may raise. To achieve this synergy, the retailer and its partner systems must be combined to improve communication flows. This creates two problems:

1. The partner might not have prudent email marketing policies (such as outlined above in this study).
2. Consumer data might be centralized, leading to privacy concerns.⁵⁰ Centralizing data will create privacy fears because all the data gets placed into one location, leading to greater concerns should the data repository's security be breached.

To overcome these problems, the retailer should require that its partners follow prudent email marketing policies (as outlined above). To resolve the centralization problem the retailer must analyze the data. If combining the data sources does not make the whole data set any more sensitive than before, then centralization should not compromise security. A hacker breaking into such data will not discover any information that could not have been obtained by breaking into separate locations of data. If linking does bring sensitive data into a central location, separate systems should

⁵⁰ FTC: Federal Trade Commission www.ftc.gov Cited: October 9, 2000

be maintained to make sure sensitive information does not now have a better access location.

G.2. Systems Implementation

Regardless of the email marketing strategy pursued, the retailer may need to acquire new software. If its IT skills are good, then it can build the software itself. Otherwise, it can buy the software and analytical tools from companies like Xchange.com, Broadbase.com, and Epiphany.com, which specialize in targeted email marketing.⁵¹ In either case, this would involve standard software installation and maintenance costs, as well as organization issues like personnel training. Also, customer data (e.g. customer preferences on which the email campaign will be based) will have to be acquired, through the retailer's own communication channels or by purchasing brokered customer lists.

The retailer also can chose to outsource the entire effort to professional firms, if it does not wish to deal with building a system or the organizational change at that juncture. Network advertising companies such as Double click, 24/7 Media and Matchlogic provide fully integrated services such as Double click email network, 24/7 Connect and Matchlogic Deliver-e that retailers might find useful.⁵²

In either case, whether the software is purchased or outsourced to firms like 24/7 Media, multi-lingual support, integration of advertising campaigns among different channels (e.g. fax, direct mail, and personalized web content) and customer groups (e.g. B2C, B2B, etc), tracking response rates, are just some of the other services which are available, and can improve an email marketing campaign.

H. Limitations

This study was limited by several factors. First, it did not delve into the nuances of the law. For example, explaining who exactly is considered a "data subject" – the person himself, his legal guardian, the computer user, etc. – was not done, yet it could have clarified the email marketing

⁵¹ Xchane-eCRM www.xchange.com. Broadbase Software.Inc www.broadbase.com; E.PIPHANY www.epiphany.com all Cited: November 19, 2000

⁵² Doubleclick www.doubleclick.com. 24/7 Media www.247media.com; MatchLogic www.matchlogic.com all Cited: November 19, 2000

advice in this study. Perhaps greater vigilance is necessary if it is the person himself and not just the computer user. The study also did not conduct a concrete cost benefit analysis for many of its recommendations. For example, hiring a Chief Privacy Officer might require substantial expense, but it depends on the expertise necessary and on available skills on the market. Perhaps retraining an existing employee to take on new responsibilities could be a better solution. Finally, our selected set of parameters, a US retailer, Internet and wireless phone email platforms, and the US and EU -- although generalizable, may not represent all trends for future email marketing. For example, the statistics point that the retail sector contributes only 30% share of the online advertising expenditures (the highest nevertheless)⁵³. If however, in the future let us assume that the banking sector becomes the most dominant sector, then the advertising recommendations would change, since banks have different requirements. Consumer data possessed by banks (financial data) is far more sensitive than simply “customer interests,” therefore; the emails used for advertising might require more important features such as secure encryption.

I. Conclusion

Email marketing can be a productive sales channel. Email is inexpensive to send and can be highly customized for specific customers. Yet firms may overuse such flexibility and burden consumers and ISPs with UCE. To deal with the rising legal, ISP, and consumer anti-spam sentiment, firms must follow existing and pending regulations; abide by ISPs’ UCE policies; and obtain consent from consumers before starting their email campaigns. Eventually, if all firms agree to such policies, email marketing should become a well-serving promotional tool.

⁵³ Internet Advertising Bureau <http://www.iab.net/> Cited: November 3, 2000