Dealing with Unsolicited Commercial Emails: A Global Perspective

by Éloïse Gratton

Email marketing is a simple and cost-effective marketing tool used to boost traffic, promote direct marketing offers, announce a new product or service, and increase revenues. E-marketers may use cheap medium to market thousands of online users at the same time, including the ones who do not wish to be solicited. A recent spam study, conducted by pollster Ipsos-Reid, determined that spam now represents, on average, more than half of all email messages that Internet users get[1]. The exponential growth of spam is affecting consumer confidence in the Internet and may hamper the growth of e-commerce. According to a recent survey published by consumers group Trans-Atlantic Consumer Dialogue, 52 percent of respondents are shopping less on the Internet or not at all because of concerns about receiving spam[2].

Unsolicited commercial emails (or spam), considered a form of privacy violation, has become a major problem for legitimate businesses, Email Service Providers (ESPs), Internet Service Providers (ISPs), and online users that have undertaken various initiatives in an attempt to curb spam. ESP Microsoft's MSN Hotmail is now imposing rate limits on daily email usage[3]. Many ISPs, such as AOL and EarthLink, have undertaken lawsuits in an attempt to discourage spammers[4].

Spam can to a certain extent be fought by using anti-spam software, although a consequence of using anti-spam filtering software may be that some wanted emails will be filtered and lost. Various industry associations are setting guidelines on how to label email headers and subject lines accurately and are promoting e-mail marketing best practices.

Many countries have recently either adopted or introduced privacy and anti-spam legislation in order to regulate the collection and handling of personal data such as email addresses and prohibit spam. Enforcing anti-spam laws is a major challenge given that the anonymity of the Internet makes it difficult in many cases to identify the spammer. Spammers also often launch their spam attacks from outside the state or country they are doing business in.

E-marketers should be implementing and adopting anti-spam policies and best practices in order to address the decentralized and global nature of the Internet. E-marketers who deliver permission-based communications to online users based on expressed needs and interests may ultimately increase their response rate and build efficient ongoing dialogues with these customers.

ANTI-SPAM INITIATIVES AND REGULATORY FRAMEWORK

The increasing prevalence of spam has led to the development of many anti-spam software and the introduction of guidelines by several industry associations. On the legal side, many countries have recently enacted laws that regulate the collection and handling of personal data and that prohibit spam, while others have amended pre-existing laws in order to address spam issues.

WHAT IS SPAM?

The definition of spam is inconsistent among ESPs and ISPs, the direct marketing industry, spammers, and consumer groups all taking different positions. For instance, although most email users agree that pornographic material and unsolicited advertising disguised as messages from friends are undesirable, some people may

Éloïse Gratton practices corporate, commercial, and information technology law with McMillan Binch Mendelsohn, a law firm with an office in Montreal, Quebec, Canada. She can be reached at Eloise.gratton@mbmlex.com

welcome messages from brand-name retailers whose Websites they visit, which makes it difficult to enforce for consistent interpretation a definition that would be widely acceptable.

The difficulty in defining spam was also apparent in Industry Canada's 2003 report on spam[5]. Not all participants agreed with the general definition of *unsolicited commercial email*, since certain participants expressed the view that a definition should also be based on the volume and indiscriminate nature of commercial email. In Australia, the National Office for the Information Economy, when reviewing the extent of problems caused by spam, had suggested to use the following working definition of spam: *a communication that could not be reasonably assumed to be wanted or expected by a recipient*[6]. Anti-spam laws (such as the CAN-SPAM Act and the European Privacy Directives) suggest that direct marketing communications sent to recipients who have dealt voluntarily with the sender before and, on the basis of that *existing relationship*, can reasonably be assumed by the sender as being prepared to accept messages of the type being sent should *not* be regarded as spam, if certain other requirements are complied with (such as if a removal option is provided).

Spam messages usually contain one or more of the following characteristics:

1. They are sent in a largely untargeted and indiscriminate manner, often by automated means;
2. They include or promote illegal or offensive content and/or their purpose is fraudulent or otherwise deceptive;
3. They are sent after personal information, such as email addresses, are collected in breach of privacy laws;
4. They are sent in a manner that disguises the originator, often using an unauthorized use of third party's email server; and
5. They do not offer a working address to which recipients may send messages opting-out of receiving further unsolicited messages and/or the sender does not honor the opt-out request by the recipient.

Spam is an unwelcome intrusion into the online users' lives, especially when messages are provided links or pointers to Web sites with information and images that can be considered offensive or inappropriate for children. A recent survey also revealed that consumers feel that spam is costing them time and money[7]. The time-consuming process of deleting the unsolicited emails is added to the time taken to download spam. Furthermore, Internet users that have email wireless devices that bill them based on the amount of data that they download actually pay to receive spam. Certain users have limits on the amount of email that their ESP will hold. Spam can often mean a full mailbox, with the result of having desirable emails getting rejected.

There are many other costs that ISPs and other business have to bear due to spam such as bandwidth and network costs; downtime attributable to spam overload; clogging of computer servers of ISPs; and productivity cost to businesses caused by time taken by employees to open, read, and respond to such messages.

TECHNOLOGY INITIATIVES

Over the past few years, several ISPs have developed some spam-blocking features. One type of spam filter technology is white listing, that is, all emails from a source not in the subscriber's address book are refused. An authentication request is sent back to the source, and only emails from people who respond to the request 9machine-generated email will not reply to the challenge) get placed in the user's inbox. Although generally considered effective, the side effects of this technology are an increase in transmission costs since it generates additional messages in response to spam received and the fact that it might offend friends and business associates trying to contact the user.

A second type of anti-spam software is the blacklist technology designed to

keep track of known spammers by relying on a network of online users who report spam to a central database, which then updates everybody's filters that would block spammers. A key drawback of this technology is that it might flag legitimate organizations or e-marketers as spammers. In December 2001, several official acceptance email letters sent by Harvard University to its freshmen were never received because these emails were filtered out as spam by the anti-filtering software used by AOL[8]. A third type of anti-spam software is called a Bayesian filter, which is a trainable program that analyses the emails that the user labels as junk. Over time, this system will build a profile that screens out most of what the user does not seem to need or read. The software holds all the mail in a separate folder so that the recipient can review the email messages that have been filtered before deleting them.

Certain electronic mail systems allow online users to view the sender and subject line of an electronic mail, and also to delete the message, without having to download the rest of the electronic mail's content or any attachments. This can reduce costs resulting from downloading unsolicited electronic mails or attachments and the European Directive 2002/58/EC suggests that these types of arrangements are useful and can serve as an additional tool to the general privacy obligations of organizations.[9]

While anti-spam filters are not perfect, they can significantly reduce the amount of spam received. The downside of email spam filters is that they require additional cost in time (human intervention is often required to scan filtered email), as well as the risk of losing important messages.

INDUSTRY INITIATIVES

Several industry associations comprised of ISPs, e-marketers, and legitimate ESPs have published privacy guidelines in an attempt to use self-regulation to protect online users' privacy and fight against spam. The Coalition Against Unsolicited Commercial E-mail (CAUCE) is a US-based non-profit organization with affiliations in Europe, Canada, Australia, and India of more than 40,000 Internet user members. It promotes legislation to outlaw unsolicited commercial email and favour the opt-in model, whereby an email message is sent only with the user's prior express consent.

The Network Advertising Initiative (NAI) is an organization formed in November 1999 to develop a framework for self-regulation of the online profiling industry. NAI has been recently focusing on the growing problem of spam, and as part of this effort, a coalition known as the E-Mail Service Provider Coalition (ESPC) has been formed within the NAI to represent the interests of ESPs. The ESPC supports the introduction of strong federal legislation to respond to the growing menace of spam.

The Direct Marketing Association (DMA) is the largest trade association for businesses interested in direct, database, and interactive global marketing, with approximately 4,700 member companies from the United States and 53 other nations. In April 2002, the DMA published guidelines aimed at providing individuals and organizations involved in direct marketing with generally accepted principles of conduct[10]. The Association for Interactive Marketing (aim), A DMA subsidiary, is a non profit organization founded in 1993 and devoted to helping marketers use interactive opportunities to reach their respective marketplaces. The AIM also recently issued guidelines to promote the most effective and ethical use of email[11]. The Canadian Marketing Association (CMA), the largest marketing association in Canada with members such as Canada's major financial institutions and insurance companies, has a code of ethics designed to set and maintain standards for the conduct of information-based marketing in Canada.

LEGAL INITIATIVES AND FRAMEWORK

Organizations buying, selling, or leasing electronic mailing lists, which are the basis for bulk unsolicited electronic emails, are subject to the provisions of law regulating the collection and use of personal information. E-marketers looking to send commercial email messages are also covered by anti-spam legislation.

Canada

In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA)[12] requires businesses to offer Canadian citizens certain guarantees regarding the collection and use of personal data such as email addresses. Many Canadian have introduced privacy legislation that would affect the legal sector, although earlier this year, the Quebec government filed a constitutional challenge in connection with PIPEDA.

Canadian policy on spam was initially articulated in 1999 in an online policy document from Industry Canada's electronic commerce branch[13]. It suggested that specific anti-spam legislation was not needed (given that spam could in some cases be fought by existing laws such as the criminal code, the *Telecommunications Act*, and PIPEDA). With the significant rise in the volume of junk email experienced in 2000 and 2001, it published in January 2003 another discussion paper entitled "E-mail Marketing: Consumer Choices and Business Opportunities" that raises different discussion points on the responsibility of ISPs, the value and role of filtering technologies and anti-spam policies, and the role of governments[14]. A few anti-spam bills were proposed in Canada in the past months and have received first readings. Canada's industry minister is considering legislation to fight unsolicited emails[15]. Industry Canada developed in 2003 the voluntary Canadian Code of Practice for Consumer Protection in E-Commerce[16], aiming to establish standards for e-commerce and commercial e-mail.

United States

In the United States, the safe harbour agreement[17], adopted on November 1, 2000, was designed to provide legal protection to US companies and organizations that, as part of their European operations, gather PII about people living there and to adequately meet the European Union's data privacy directives, which are more stringent than current US privacy law. The *Children's Online Privacy Protection Act*[18] applies to the online collection of personal information from children under 13. On the anti-spam side, the *CAN-SPAM Act*[19], introduced on April 10, 2003, by Ron Wyden and Conrad R. Burns, took effect as of January 1, 2004. This bill has been criticized as being too weak and superseding stronger US state laws. Europe is blaming the weak US laws for most of the spam in Europe[20].

Europe

In Europe, the collection and handling of personal information such as email addresses and unsolicited commercial emails are regulated by the privacy Directives 95/46/EC and 2002/58/EC. This last directive required implementation in member states by the end of October 2003. The United Kingdom has since passed anti-spam legislation.

International: OECD Guidelines

On an international level, the collection and handling of personal information is regulated by the 1980 set of practices[21] developed by the Organization for Economic Cooperation and Development (OECD). These principles are commonly referred to as the code of Fair Information Practices and are the basis of several privacy laws around the world, including Canadian PIPEDA and the US safe harbour agreement. Recently, to make it easier for member governments to collect evidence and practical help from foreign agencies and to otherwise increase international cooperation in the prosecution of spammers and other cross-border frauds, new suggested guidelines for protecting consumers from cross-border fraud have also been published by the OECD.[22]

ADOPTING ANTI-SPAM BEST PRACTICES

The use of the Internet to send large volumes of email to promote products and services affects the facilities of ISPs and also hurts the business of legitimate e-marketers. If online users become overwhelmed by irrelevant solicitations by email, they may quickly develop a bitter taste for legitimate e-marketers. E-marketers should adopt anti-spam best practices to build and ongoing, mutually beneficial relationship with recipients through email marketing.

DISCLOSING THE UNSOLICITED EMAIL POLICY

Online users often voluntarily provide their email addresses to Web sites in the context of Web site registrations or when purchasing an item from an e-commerce Web site. Internal or external secondary uses, such as marketing back to the user or selling a list of email addresses to third parties, may go beyond the use for which the information was initially provided by or collected from the online user.

The Center for Democracy and Technology (CDT), a non-profit organization that works to promote democratic values and constitutional liberties in the digital age, recommends to online users not to provide their email addresses to a Web site unless the site offers the option of declining to receive email messages and enables the users to exercise that option[23]. The Canadian Code of Practice for Consumers Protection in Electronic Commerce recommends that the online vendor's policies on privacy and unsolicited email information be available to consumers before they engage in transactions[24]. On the industry side, the DMA suggests that consumers providing their personal data be informed periodically by marketers about their policy concerning the rental, sale, or exchange of such data[25]. It also suggests that the opportunity to opt out of the marketing process be provided to online users. CMA, that provides for a similar requirement, suggest that this opportunity to decline to have their name or other information transferred or used for any further marketing purposes by a third party be repeated once every three years, at a minimum[26].

E-marketers should provide online users with their policies on unsolicited email before or at the time that online users engage in a transaction or provide their personal data. The anti-spam policy should be included in the Web site privacy policy, which should be available on the homepage of the Web site before the online user registers to the Web site or finalizes an online purchase. The AIM suggests that e-marketers also adopt policies relating to other issues such as reply handlings, the processing of and time frames relating to unsubscribe requests by recipients, and the suppression of known invalid addresses[27]. The goals of this list hygiene policy should be to reduce incorrect, incomplete, or outdated addresses; to process remove requests promptly; and to inform online users how long it will take for an opt-out request to be effective. This may help set appropriate customer expectations, thereby limiting customer complaints relating to spam.

AVOIDING ILLEGAL COLLECTION AND USE OF EMAIL ADDRESSES

An e-marketer usually obtains an extensive list of email addresses to launch its commercial mailing campaign. In building such list, these marketers may use the resources available on the Internet, purchase a list from a third party, or collect email addresses directly from online users. In October 2002, the Privacy Commissioner of Canada criticized several large Canadian communication companies for failing to obtain meaningful consent from their customers before using their email addresses for secondary purposes such as commercial solicitation[28].

Although *business* email addresses are in certain cases either not regulated by privacy legislation (in certain Canadian provinces and in the United Kingdom) or their status is unclear (PIPEDA), email addresses are usually considered personal information. Canada's PIPEDA[29] or the US

Children's Online Privacy Protection Act[30] would regulate the collection of email addresses (or at least of *personal* email addresses), and in Europe, Directive 95/46/EC also has a very broad definition of *personal information* that would most likely include email addresses[31]. On the industry side, the NAI also concluded that PII (personally identifiable information) includes email addresses[32]. The DMA, which usually adopts a more liberal stance on the issue of promotional email, encourages its members to indicate to online users at the moment of collection how an email address could be used[33]. Certain types of email address collection may be illegal pursuant to privacy laws or industry guidelines.

INFORMATION VOLUNTARILY PROVIDED BY ONLINE USERS

An online user's email address may, in some cases, be provided voluntarily by the user such at the time of registering to a Web site or upon purchasing items from an e-commerce Web site. A privacy breach might occur if the email address collected is then used or transferred for a purpose not disclosed at the time of the collection. As an example, it was reported in December 2002 that MP3.com required users to provide an email address before they could listen to music. Subsequently, without disclosing to the online users what will happen with the data collected or offering a choice or notice, the site provided that address to six mailing lists, including a music newsletter and another one for *partner product announcements*.

E-marketers should not assume that online users that have provided personal data such as their email addresses in the context of Web site registration or online purchases expect that their email addresses will be used for other purposes, although it is generally accepted that a previous business relationship may entitle an e-marketer to contact this user for offering an advertisement upon certain requirements. On this issue, the recent European Directive 2002/58/EC indicates that, in the case when electronic contact details are obtained, the customer should be informed about their further use for direct marketing in a clear manner and be given the opportunity to refuse such usage[34].

In order to avoid breaching online users' privacy, e-marketers that initially collect personal data in the context of a Web site registration or a transaction should disclose whether they intend to use this data for other purposes such as marketing back to the user and provide these users with the opportunity to refuse such marketing.

PURCHASE OF THIRD-PARTY LISTS

Once an e-marketer identifies the audience for a specific advertising campaign, the next step is to build an email subscriber list. There are a number of companies that work as list brokers and that are selling lists containing millions of email addresses at very low prices. Online users are becoming more concerned about the transfer of their personal information. A study conducted by AT&T noted that, when deciding whether to provide information to Web sites, respondents reported that the most important factor was whether their information would be shared with other organizations.[35]

Although it could be impractical for a direct-marketing firm that wishes to acquire a mailing list from another organization to obtain prior consent from online users, the organization providing or selling the list to the third-party direct-marketer would be expected to obtain consent from the online users before disclosing their personal information. The general concept entails that online users should provide their consent prior to the collection of their data and also prior to secondary uses of their personal data[36]. Therefore, organizations that are transferring customer email address lists should obtain customer's consent before transferring the addresses to a third-party purchaser of the marketing list.

ONLINE TRACKING TOOLS

One way to collect personal information of online users is through online tracking tools such as cookies, which are small pieces of code transferred from a Web site to a home computer when a user is surfing or visiting a Web site. Some more recent technologies such as Web bugs (or special links in Web pages) used by e-marketers to validate email addresses are also raising privacy concerns since they can be used to track down the activities of an online user and gather information about the user through its computer. Recently, *spyware* software, usually downloaded into a computer when the user downloads free software from the Internet, has emerged. Spyware gathers information about the online user's Web-browsing habits or e-commerce data and then relays the data to a third-party company.

In Canada, the Privacy Commissioner concluded that information stored by cookies usually qualifies as personal information for the purposes of PIPEDA and that the use of cookies should be disclosed to online users. Directive 2002/58/EC is clear on the fact that online users should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment[37]. Online users should be provided clear notice about the type of information collected (such as email addresses) about them and should be informed before a placement of any such online tracking devices in their computers. They should be entitled to refuse this placement.

PUBLIC SPACES ON THE INTERNET

Another way for e-marketers to collect email addresses of online users is by gathering them from public spaces on the Internet, such as public email directories, emailing lists, news groups, or even chat rooms. In the summer of 2002, the CDT set up hundreds of different email addresses, used them for a single purpose, and then waited six months in an attempt to determine the source of spam. The major findings of the study on spamming tactics, entitled "Why Am I Getting All This Spam?", was that email addresses posted on Web sites or in newsgroups attracted the most spam[38]. Another spam study published by the Federal Trade Commission (FTC) revealed that 100 percent of the email addresses posted in chat rooms received spam; the first was received only nine minutes after the address was posted.[39]

Certain tools available on the Internet help marketers collect email addresses. These programs will search Web sites, which have to be specified in advance by a list of URLs, or keywords related to a predefined field of interest and, subsequently, will provide all email addresses found on the Web sites and pages. Anti-spam legislation such as the CAN-SPAM Act bans sending commercial email to addresses that were gathered *using automated means*[40]. On the industry side, AIM guidelines suggest that e-marketers should not harvest email addresses with the intent to send bulk unsolicited commercial email without consumers knowledge or consent. "Harvest" is defined as compiling or stealing email addresses through anonymous collection procedures such as via a Web spider, through chat rooms, or from other publicly displayed areas listing personal or business email addresses.

The practice of collecting email addresses from public spaces on the Internet and using them for commercial e-mailings constitutes unfair processing of personal data and would go against the *purpose* principle. Online users usually disclose their email addresses for a specific purpose, such as participating in a newsgroup, this purpose being different from commercial emailing. E-marketers should therefore avoid collecting email addresses from public places on the Internet.

MAIL SERVER ATTACKS

In February 2003, Microsoft filed a suit in the federal court for the northern district of San Jose, CA, accusing the anonymous defendants of using a dictionary attack to discover active Hotmail ac-

counts[41]. Spam is in certain cases generated through attacks on mail servers, methods that do not rely on the collection of email addresses at all. In these types of attacks, also known as brute force attacks and dictionary attacks, spam is sent to millions of random email addresses (every possible combination of letters at a domain or to common names and words) to see which ones are active. The DMA announced at the FTC 2003 spam workshop its position against this practice[42]. Although in this case, there is no illegal email address collection *per se*, email addresses should not be used for email marketing purposes without the online user's prior consent.

OBTAINING CONSENT

E-marketers should generally offer online users choice and consent as to the use of their e-mail addresses, especially if such use goes beyond the use for which the information was provided, obtained, or described in their privacy policy. E-marketers should only send commercial emails to online users with whom they have a pre-existing relationship or when prior consent has been obtained.

THE NOTION OF "PRE-EXISTING RELATIONSHIP"

Commercial emails should not be considered unsolicited if the e-marketer has an existing or prior relationship with the online user. This principle is accepted by the recent European Directive 2002/58/EC[43], the CAN-SPAM Act and promoted by the Canadian Code of Practice for Consumer Protection in Electronic Commerce[44], as well as industry guidelines. The key issue is related to the definition of a pre-existing business relationship between the e-marketer and the online user, given that although marketers have every incentive to define the term loosely, online users may have a different interest.

On the industry side, the AIM defines a prior business or personal relationship as any previous correspondence, transaction activity, customer service activity, personalized marketing message, third-party permission use, or proven offline contact[45]. An application or request for information initiated by the individual may also qualify. The DMA's guidelines suggest that a previous business relationship also may be established responses by the individual to questionnaires or surveys and responses to sweepstakes or contests[46]. In Canada, the CMA states that a current customer is defined as any consumer who has made a purchase from the marketer within the last six months or during a normal buying cycle[47]. In the United States, the CAN-SPAM Act limits an existing relationship to an activity that took place within three years of the sending of the commercial email[48]. The period of three years could be viewed as a long period and has been criticized by certain authors.[49]

Online consumers should not be solicited by e-marketers they do not know, unless they have already agreed to be solicited by such marketers. An existing relationship is not established by consumers simply visiting, browsing or searching a Web site. E-marketers should not assume that simply because an individual has purchased something from them that he/she automatically consents to being solicited with commercial emails.

OPT-IN VS. OPT-OUT

Commercial emails should not be unsolicited and permission can be obtained in a number of ways. The main issue relating to the consent is whether online users, assuming that they do not have any previous business relationship with an e-marketer wishing to solicit them, should provide affirmative consent (or opt-in) to any emailing list used for advertising purposes or opt-out from the list.

The AIM suggest that affirmative consent or opt-in would provide a more highly qualified level of permission from consumers. This would include (1) the double opt-in consent: once an online user has elected to receive email commercial messages, a confirmation e-mail is then sent to the user to which he/she must reply

(by replying to the message or clicking on a URL contained within) before the list owner may add them to their list; (2) the confirmed opt-in consent: once an online user has elected to receive email commercial messages, a confirmation email is sent which would include the opportunity to remove their subscription; and (3) the simple opt-in consent: a user has actively elected to receive email commercial messages by using any method such as checking an opt-in box.

A simple consent would include the opt-out method, whereby an online user must request not to be included on an email list at the point of collection or with subsequent communications, using the removal option from mailing lists. Opting out is usually the favored method by direct marketers for obvious reasons. Ray Everett-Church, founder of the consumer group CAUCE, believes that the opt-out provision provides spammers free rein and that an opt-out policy will not significantly reduce the widespread damage to consumers.[50]

There are many issues with an opt-out system, since it is used by spammers inconsistently and often worsens the problem. Many victims of spam receive a significant volume of email that makes it difficult and time-consuming to opt-out. E-mail addresses accumulated by spammers are often obtained from the common use of the Internet and usually increase in value when recipients respond to opt-out. Spammers use these confirmed and active email addresses to resell them at higher values by packaging them as online users that actually read their emails and took the time to respond. In addition, recipients that have multiple email addresses, such as businesses, find it difficult to identify which email address is the one used by the spammers. A recent survey released by Transatlantic Consumer Dialogue, a group of European and US consumer organizations, found that 81 percent of respondents in both areas supported laws requiring permission (opt-in) before sending commercial email[51].

It has been suggested that marketers who implement affirmative consent permission practices generally have higher response rates and lower complaint rates and blocking issues[52]. A study from the Commission of the European Communities on unsolicited commercial communications and data protection concluded that major e-marketers and direct marketers were switching to an opt-in approach[53]. It is increasingly common to find in a marketing email some type of statement that the message has been sent to the user because the user has opted in to receiving it. Opting in or any method associated with affirmative consent would be an effective alternative, since it addresses most of the issues associated with spam. This permission is usually obtained by providing an application and agreement form on a Web site.

In the United States, the CAN-SPAM Act has taken an opt-out approach, while the European Union's recently enacted directive 2002/58/EC forbids unsolicited commercial email unless with the recipient's prior consent (through an opt-in mechanism). E-marketers in opt-out countries might target email addresses not only within their own country but also to consumers in other countries with an opt-in system. Since email addresses do not often provide an indication of the recipient's country of residence, an inconsistent global system will not provide a common solution for the protection of an online user's privacy. Opting in is a well-balanced and efficient solution to remove obstacles to the provision of commercial communications while protecting the fundamental privacy right of online users.

THE CONTENT OF THE CONSENT

When gathering online users' consent prior to sending commercial email messages, e-marketers should inform the recipient about the nature and type of email messages that he/she will receive, such as the type of advertisement, offer, or product that will be sent. The frequency of those communications also should be disclosed. E-marketers should track and record all customer permissions, and the date and time received, in order to expe-

dite responding to inquiries[54]. They should review inactive customers carefully and consider reconnecting offline with them.

Online users should, upon request, be provided with information including when their consent/permission was granted or disclose the details of the relevant previous business relationship (including details and the extent of that relationship). For many organizations, having the evidence of the consent at their fingertips in order to be able to show to the requesters the details of this consent can be an onerous task. On the technical side, SmartConsent, a software developed by Canadian software provider Smartech Consulting Inc., stores the digitized consent evidence and other relevant information, such as the date and time when the consumer's consent was granted, in an encrypted electronic repository. With a few key strokes, the details relating to a consent can be retrieved using a secured Web browser.

LABELLING ISSUES

Identifying the Subject and Content of the E-Mail

The FTC recently issued a report on the false claims in spam in which it concluded that, in the 1,000 spam messages reviewed, 66 percent contained false from lines, subject lines, or message text[55]. Many spammers are including misleading information in the message's subject lines in order to include the recipients to view the messages.

On the industry side, guidelines suggest that the solicitations sent online should be clear, honest, and not misleading[56]. The subject line should accurately reflect the message, purpose, and content. E-marketers should avoid potentially using deceptive prefixes in the subject line, such as "RE" or "FW", and the content of the message should clearly describe the offer and its benefits to the recipient[57]. The CAN-SPAM Act makes it unlawful to send a commercial electronic mail message that contains header information or subject heading that is false or misleading[58].

AIM suggests that e-marketers should pre-test creative elements and content with anti-spam software to avoid words, phrase, coding, punctuation, and design common to spam[59]. Given that certain efforts to block spam using anti-spam filters also end up blocking good email, spammers are trying to modify their messages to get through and are increasingly trying to make their emails not look like spam. For instance, because some spam filter software scan for certain keywords, such as free, which indicate that it may be spam, typing the word fr*ee could outsmart the filter software. Some try not to use trigger words, such as Free., No Cost, Win, and ensure not to use excessive punctuation, such as question marks, exclamation points, or percentage signs, since many anti-spam software may detect it and block it.

Although e-marketers may wish to ensure that their messages will not get blocked by anti-spam software, they should identify the subject line and body text to accurately reflect the content and purpose of the email. Communications should contain only the type of content described in the notice the customer originally received and agreed to or content relevant to the pre-existing or current business relation.

Identifying the Source of the Email

An increasing number of spammers include misleading information or disguise the source of their commercial email to prevent recipients from responding to such mail quickly and easily. This practice of disguising or concealing the identity of the sender is prohibited by the European Directive 2002/58/EC and the CAN-SPAM Act. Header information that is technically accurate but includes an originating electronic mail address unauthorized or obtained by fraudulent representations is considered misleading.

On the industry side, the DMA and the AIM guidelines state that solicitations sent online should disclose the marketer's identity. On the technical side, many industry players are building solutions that may help consumers effectively avoid spam, a

challenge that certain current anti-spam software fail to address. The E-mail Service Provider Coalition (ESPC) recently announced a blueprint code-named Project Lumos, a registry-based model developed to eliminate spam by holding senders accountable for the mail they send[60]. Project Lumos uses a certification process that makes it impossible for high-volume mailers to conceal their identities; a verification process that ascertains the mailer's identity, thereby facilitating transparency a process that requires standardization of all sender information in the mail header, including the use of an identifiable, traceable unsubscribe URL; an authentication process that provides secure proof of sender identity; and a process that captures, monitors, and reports performance data for all senders and mailers.

Yahoo! has also proposed a new ID tool known as DomainKeys that would establish email senders' identities to ensure that spammers are unable to hide the origin of their messages[61]. This tool, available to domain owners and receivers, would enable domain owners to create a public and private key. Email sent from the domain would have a digital signature in the header containing the private key. Receivers would match up the private key with a public key registered with the Internet domain name system, therefore entitling ISP using this system to establish the sender's identity. ISPs also could block senders that would fail or refuse to establish their identity. TRUSTe is fighting spam by launching its Trusted Sender program that places a seal on an email that identifies the commercial sender as legitimate and practicing responsible email marketing[62]. An email sender earns the Trusted Sender label if it accurately identifies itself, the topic of the email, and the actual address from which it was sent.

The falsification of electronic source, the Internet domain header information, date or time originating email addresses, or other email identifiers for the purpose of concealing the origin of any bulk email should be prohibited and avoided by all e-marketers. Commercial emails should clearly display the name, and the email and physical postal address (no PO boxes) of the distributor of the email and the marketers of the products advertised. This information should be made available in the email solicitation or by the link to the marketer's Web site. E-marketer's brand should be prominent in the from line and/or the subject line. Each email communication should be time-and-date-stamped in the header or email body to indicate when the communication was sent/received.

PROVIDING AN OPT-OUT MECHANISM

Some senders of unsolicited commercial electronic mail messages provide simple and reliable ways for recipients to reject (or opt out of) receipt of unsolicited commercial electronic mail from such senders in the future. Unfortunately, other senders provide no such opt-out mechanism, refuse to honor the requests of recipients not to receive electronic mail from such senders in the future, or both.

Adequate Removal Method

Online users should be allowed to opt out of any emailing list used for advertising purposes, regardless of whether they have previously opted in or not. European and US anti-spam legislation and industry guidelines are unanimous on this issue.

The head of the CMA suggests that the option to opt out is often hard to find, the language is difficult to understand, or the process is too time consuming[63]. Also, an Ekos study demonstrated that opt-out approaches are considered acceptable only if the opt-out provision is brought to the customer's attention, is clearly worded, provides sufficient default, and is easy to execute[64]. The mechanism for opting out should be clear and in a location that is easy to locate such as the first text in the body of the message or at the complete bottom of the email. Such remove option should be in type that is easy to read, of the same size as the majority of the text of the message or in bold, and understandable and simple enough to ensure that consumers are aware of and understand the option being offered. The opt-out procedure should be included in

the email to enable online users to opt out online.

In many cases, an email address or URL is put at the end of each marketing message clearly identifying that, in order to unsubscribe to the email list and stop receiving messages from the e-marketer, users should reply to this email address link with the word unsubscribe in the subject title. A confirmation may be sent by the e-marketer that the opt-out message has been received and that the user will be removed from all lists. The unsolicited email also could include a statement informing the recipient of the tool-free telephone number that the recipient may call or a valid return address to which the recipient may write or email, as the case may be, notifying the sender not to email the recipient any further unsolicited documents to the email address, or addresses, specified by the recipient. The opt-out procedure should be free of charge[65].

E-marketers should ensure that the email address to which online users would reply is a valid one or that the URL or the other Internet-based mechanism offered to opt out is functional for a period of 30 days after the transmission of an email message. US anti-spam legislation provides that a return electronic mail address or other mechanism does not fail to comply with the opt-out requirements if it is unexpectedly and temporarily unable to receive messages due to technical or capacity problems and if the problem with receiving messages is corrected within a reasonable time[66]. This may open the door for spam, since spammers that have not honoured an opt-out request could claim that their opt-out inbox was temporarily full in order to defend themselves against a spam complaint.

The fact that an online user must provide personal information to opt out may raise additional privacy issues. E-marketers should not request that online users provide personal information to be removed from marketing lists.

Honoring the Requests of Users to Opt Out

E-marketers should not violate their own privacy policies, although it might be frustrating to be unable to contact online customers once the user has selected to opt out. An AT&T study concluded that online users consider as an important factor whether a Web site will remove them from their mailing lists upon request[67].

As part of the Trusted Sender program, the sender should have transparent policies for allowing recipients to remove themselves from the emailing list. Many abusive emailers or marketers appear to provide recipients with an option of having their names removed from some type of mailing list and/or provide a link to "unsubscribe here" in their email marketing messages. Instead, these marketers are either using the reply as a means of validating an email address or are using Web bugs to know that a certain email message has been opened. In this case, the consumer who replies or opens a spam email is likely to get more commercial solicitation. Some spammers simply ignore the request or even provide an invalid email address to unsubscribe. A FTC study concluded that 63 percent of the removal requests were not honored[68].

Certain e-marketers could be tempted to make certain exceptions that violate their own privacy policies. In 2002, Lycos ignored members who explicitly opted out of receiving special offers. In this case, Lycos revised its special offer program and created a $5,000 sweepstakes prize in the hopes of convincing those who had opted out to change their minds and sent an email with a link that automatically resent recipients' settings to opt in when online users clicked on it[69]. Lycos argued that the sweepstakes constituted a special one-time offer to Lycos customers. E-marketers should not contact online users who have opted-out from future commercial emails unless this contact is only to confirm the opt-out request has been received and is being acknowledged.

The issue of timing is addressed by the DMA[70], without specifying what should be considered as "timely". The AIM guide-

lines suggest to process *online* remove requests immediately and to process remove requests received *offline* within 10 business days[71]. The CAN-SPAM Act also considers a period of 10 business days as appropriate, whatever the removal method used[72]. Opt-out or unsubscribe requests should be honoured on a timely basis and if possible, immediately upon the reception of the opt-out request using real-time removal procedures. The e-marketer should detail in the opt-out procedure the period that it needs to honor the user's opt-out request.

Once the e-marketer obtains an opt-out request from a user who does not wish to be contacted again by that sender, one needs to determine how long should the opt-out request should be valid. Anti-same bills introduced in the United States in 2003 that will not become law were suggesting that the opt-out request be valid for five years or for three years beginning 10 business days following the reception of the opt-out request.

Some industry observers believe that an opt-out request should not expire. The period for honouring an opt-out request is therefore still open for discussions. In the best case scenario, this request would never expire unless there is a business transaction (or any other activity that would be qualify to be a business relationship) between the online user and the e-marketer, with such transaction being initiated by the online user.

CONCLUSION

Anti-spam activists favoring anti-spam laws believe technology improvements and anti-spam software will not alone address spam issues since technology alone will not be able to hold spammers accountable but that the law will. On the other hand, the anonymity of the Internet may sometimes make it difficult to track down the source, therefore making anti-spam laws ineffective if spam victims are in no position to enforce these laws. The FTC has recently asked US Congress for new powers that would let it cooperate closely with other governments and prosecute domestic and overseas spammers more readily[73]. The FTC would be granted with the power to serve secret requests for subscriber information on ISPs, peruse FBI criminal databases, and exchange sensitive information with foreign law enforcement agencies.

On an individual basis, e-marketers, in order to distinguish themselves from spammers, can develop business practices relating to the handling of personal information in an ethical manner. They should properly disclose to their customers what their unsolicited email policy is and undertake to avoid illegally collecting email addresses. They should ensure that they respect the interests and choices of customers by only sending email advertisements to users who have either agreed to receive such marketing or with whom the e-marketer has a pre-existing relationship. In addition, e-marketers should ensure that their marketing messages indicate the name of the distributor and disclose the identity of the marketer and the content of the message in the subject title, while providing the online user with an adequate procedure to opt-out.

NOTES

[1] The study noted that the average recipient of spam receives 123 emails each week, of which 52 percent are unsolicited. See Tyler Hamilton, "Got spam?" Getting more spam? Sick of spam?", *Toronto Star*, June 12, 2003.

[2] Lisa Jucca, "Spam drives wary shoppers from Internet", *Reuters* (U.K.), Feb., 2, 2004.

[3] Stefani Olsen, "Hotmail restricts outgoing messages", *CNET News*, Mar. 24, 2003.

[4] Microsoft, "Spiking the Spammers", Feb. 12, 2003. *www.microsoft.com/issues/essays/2003/02-12spam.asp* (last accessed on June 5, 203); Roma Luciw, "Microsoft lawsuits target spammers", June 17, 2003, *The Globe and mail*; Christopher Sanders, "AOL settles spam case", April 3, 2002, Ecommerce, Internetnews.com; and Margaret Kane, "EarthLink wins spammer suit", July 19, 2002, *News.com*

[5] Industry Canada (The Working Group on Consumers and Electronic Commerce), "E-mail marketing: Consumer Choices and Business Opportunities", Discussion Paper, Jan. 2003

[6] The National Office for the Information Economy, "Spam Interim Review Report", 2002

[7] Nearly 53 percent of respondents indicated that dealing with spam places a burden on their individual time, and 36 percent feel spam imposes unwanted costs in the form of connection time, server, and disk

storage space. See Symantec Corp., "Symantec Poll: Spam Puts Canadians at Risk", News Releases, May 20, 2003.

[8] Abby Williams, "Truth finally brought to light, Harvard acceptance letters discovered unkosher", *Daily Princetonian*, Feb. 15, 2002; and IEEE Spectrum Online, "Harvard acceptance letters rejected by AOL", Jan. 2002.

[9] Section 44 of the Preamble, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), European Union (July 12, 2002).

[10] Direct Marketing Association, "Guidelines for Ethical Business Practice", Apr. 2002

[11] See Association for Interactive Marketing, "The CRE's 6 Resolutions for Responsible E-mailers", and more recently "E-mail Delivery Best Practices for Marketers and List Owners" (Council for Responsible E-mail), 2003

[12] Personal information Protection and Electronic Documents Act, c.5 (2000) (Canada)

[13] Industry Canada, (The Working Group on Consumers and Electronic Commerce), "Internet and Bulk Unsolicited Electronic Mail", July 1999.

[14] Industry Canada (the Working Group on Consumers and Electronic Commerce), "E-mail Marketing: Consumer Choices and Business Opportunities", Discussion Paper, Jan. 2003.

[15] CBC News, "Canadian anti-spam law may be in works", Feb. 4,2 004.

[16] Industry Canada, Canadian Code of Practice for Consumer Protection in Electronic Commerce, Jan. 2003.

[17] US Department of Commerce, Safe Harbor Agreement (Nov. 1, 2000).

[18] The Children's Online Privacy Protection Rule, 16 C.F.R. Part 312.

[19] CAN-SPAM Act of 2003, S. 977, 108th Congress, 1st Session (2003).

[20] Brandon Mitchener, "Europe Blames Weak U.S. Laws for Surge in the Region's Spam"*, Wall Street Journal*, Feb. 3, 2004.

[21] OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Sept. 23, 1980).

[22] OECD, Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders (June 11, 2003).

[23] Center for Democracy & Technology, "Why Am I Getting All This Spam?", Unsolicited Commercial E-mail Research Six Month Report, Mar. 2003.

[24] Principle 1.3(h), Canadian Code of Practice for Consumer Protection in Electronic Commerce (The), Working Group on Electronic Commerce and Consumer, Approved in Principle, Jan. 2003.

[25] Article 30, Direct Marketing Association, "Guidelines for Ethical Business Practice", Apr. 2002.

[26] Principle 1.1, Canadian Marketing Association, "Code of Ethics & Standards of Practice", 2003.

[27] Recommendation 4, "E-mail Delivery Best Practices for Marketing and List Owners", The Association for Interactive Marketing (Council for Responsible E-mail), 2003.

[28] Industry Canada (The Working Group on Consumers and Electronic Commerce), "E-mail Marketing: Consumer Choices and Business Opportunities", Discussion Paper, Jan. 2003.

[29] Personal information is defined as "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization". See article 2(1), Personal Information Protection and Electronic Documents Act, c.5 (2000) (Canada).

[30] Section 6502(b)(1), The Children's Online Privacy Protection Rule, 16 C.E.R. Part 312, Nov. 3, 1999.

[31] Article 2(a), Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, European Union (Oct. 24, 1995).

[32] Network Advertising Initiatives, "Self-Regulatory Principles For Online Preferences Marketing by Network Advertisers".

[33] David F. Gallagher, "Enter Maze, and Find the Opt-Out Cheese", *NY Times*, Dec. 9, 2002.

[34] Section 41 of the Preamble and article 13(2), Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), European Union (July 12, 2002).

[35] Lorrie Faith Cranot, "Beyond Concern: Understanding Net Users' Attitudes About Online Privacy", AT&T Labs-Research Technical Report TR 99.4.3, Apr. 14, 1999.

[36] Schedule I, Section 5, Article 4.2.4, Personal Information Protection and Electronic Documents Act, c.5 (2000) (Canada); Article 2, US Department of Commerce, Safe Harbor Agreement (Nov. 1, 2000); Article 6(1)(b) and Article 26(1)(a), Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, European Union (Oct. 24, 1995); Section 41 f the Preamble and article 13(2), Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), European Union (July 12, 2002); Article 10(a), OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Sept. 23, 1980).

[37] Preamble, Section 25, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), European Union (July 12, 2002).

[38] In its study, CDT discovered that most newsgroup-related spam was sent to the address in the message header, even if other email addresses were included in the text of the posting, Center for Democracy & Technology, "Why Am I Getting All This Spam?" Unsolicited Commercial E-mail Research Six Month Report, Mar. 2003

[39] Federal Trade Commission, Bureau of Consumer Protection, "E-mail Harvesting: How Spammers Reap What You Show", *FTC Consumer Alert*, available at *http://www.ftc.gov/bcp/online/pubs/alerts/spamabt.pdf* (last accessed on June 23, 2003).

[40] Section 5(b)(t)(A), CAN-SPAM Act of 2003, S. 877, 108th Congress, 1st Sess. (2003).
[41] Microsoft "Spiking the Spammers", Feb. 12, 2003, available at *www.microsoft.com/issues/essays/2003/02-12spam.asp* (last accessed on June 5, 2003).
[42] Ken Magill, "Tensions Surface Early at FTC Spam Forum", *DM News*, May 1, 2003.
[43] Section 41 of the Preamble and article 13(2), Directive 2002/58/EC Concerning the Processing of Personal Data in the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), European Union (July 12, 2002).
[44] Principle 71., Canadian Code of Practice for Consumer Protection in Electronic Commerce (The), Working Group on Electronic Commerce and Consumer, Approved in Principle, Jan. 2003.
[45] Association for Interactive Marketing, "The CRE's 6 Resolutions for Responsible E-mailers".
[46] Direct Marketing Association, the "DMA Guidelines for Ethical Business Practice", Apr. 2002
[47] Principle 3, Canadian Marketing Association, "Code of Ethics & Standards of Practice".
[48] Section 3(9)(A) and (B), CAN-SPAM Act of 2003, S. 877, 108th Congress, 1st Session (2003).
[49] Cameron Sturdevant, "Can-Spam Act Can't", *eWeek*, June 9, 2003.
[50] Mylene Margalindan, "Multiplying Spam Spurs New Legislative Efforts", *Wall Street Journal*, June 19, 2002.
[51] Brian Morrissey, "Survey Finds Wide Support for Opt-In Spam Laws", *DM News*, Feb 4, 2004.
[52] Recommendation 1, "E-mail Delivery Best Practices for Marketers and List Owners", The Association for Interactive Marketing (Council for Responsible E-mail), 2003.
[53] Gauthronet, Serge & Étienne Drouard, "Unsolicited Commercial Communications and Data Protection – Summary of Study Findings", Commission of the European Communities, Internal Market DG – Contract no. ETD/99/B5-3000/E/96, Jan. 2001, p.62.
[54] Recommendation 1, "E-mail Delivery Best Practices for Marketers and List Owners", The Association for Interactive Marketing (Council for Responsible E-mail), 2003.
[55] Federal Trade Commission, "Division of Marketing Practices", False Claims in Spam, Apr. 30, 2003.
[56] Article 36, Direct Marketing Association, "Guidelines for Ethical Business Practice", Apr. 2002.
[57] Recommendation 2, "E-mail Delivery Best Practices for Marketers and List Owners", The Association for Interactive Marketing (Council for Responsible E-mail), 2003.
[58] Section 5(a)(1) and (2), CAN-SPAM Act of 2003, S. 877, 108th Congress, 1st Sess. (2003).
[59] Recommendation 2, "E-mail Delivery Best Practices for Marketers and List Owners", The Association for Interactive Marketing (Council for Responsible E-mail), 2003.
[60] Internet Wire, "E-mail Service Provider Coalition Announces Technology Blueprint – Code Named 'Project Lumos' – Designed to Eradicate Spam", Apr. 23, 2003.
[61] Brian Morrissey, "Yahoo Proposes E-Mail I D System", *DM News*, Dec. 10, 2003.
[62] Brian Morrissey, "Yahoo Proposes E-Mail I D System", *DM News*, Dec. 10, 2003.
[63] Robert Mullins, "'Trusted Sender' Seal Aims to Weed Out the Honest E-mails From Spam", *Silicon Valley/San Jose Business Journal*, July 22, 2002.
[64] Lisa Schmidt, "Marketers Urged to Respect Privacy", *Calgary Herald*, May 30, 2002.
[65] Ekos Research Associates Inc., "Business Usage of Consumer Information for Direct Marketing: What the Public Thinks", Prepared on Behalf of The Public Interest Advocacy Center, Aug. 2001.
[66] Article 13(2), Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications(), European Union (July 12, 2002).
[67] Section 5(a)(3)(C), CAN-SPAM Act CAN-SPAM Act of 2003, S. 877, 108th Congress, 1st Sess. (2003).
[68] Lorrie Faith Cranor, "Beyond Concern: Understanding Net Users' Attitudes About Online Privacy", AT&T Labs-Research Technical Report TR 99.4.3, Apr. 14, 1999.
[69] Federal Trade Commission, "Division of Marketing Practices, False Claims in Spam", Apr. 30, 2003.
[70] Adrian Mello, "Dangerous Games With Customer Data", *ZD Net Tech Update*, July 24, 2002.
[71] Article 36, Direct Marketing Association, "Guidelines for Ethical Business Practice", April 2002.
[72] Recommendation 4, "E-mail Delivery Best Practices for Marketers and List Owners", The Association for Interactive Marketing (Council for Responsible E-mail), 2003.
[73] Section 5(a)(4)(A), CAN-SPAM Act of 2003, S. 877, 108th Congress, 1st Sess. (2003)