Managing Customer Opt-Outs in a Complex Global Environment

Matt Leonard[1], Mayra Rodriguez[1], Richard Segal[2], Robert Shoop[3]

[1] IBM Customer Relations, Policy, & Privacy, White Plains, NY, USA
[2] IBM Thomas J. Watson Research Center, Hawthorne, NY, USA
[3] Harte Hanks, Austin, TX, USA

Abstract. The day to day rhetoric associated with spam control focuses on measures, technology, rules or fees to impose order or control. These efforts concentrate on the broad range of messages throughout the internet in the hope that by reducing or stopping the flow of 'spam' the problem of spam will be solved. This is analogous to fighting a fire when it is at its apex rather than preventing it in the first place. IBM's opt-out management application, The Global E-mail Cleansing System (GECS), and the associated business process attempts to control the e-mail communications between the enterprise and its constituencies. This increases the satisfaction of its customers while ensuring that, at least in the case of IBM's communications, customers and others can feel confident that IBM is doing its best to ensure their privacy is respected.

1 Introduction

It's no secret that e-mail marketing is an emotionally charged issue. What started out as a great way to communicate, to share information, to collaborate, has instead turned into an irritating burden. Individuals feel violated by spam. Their in-boxes are swamped by unwanted messages over which they have no control. The term "Spam" has become a cry for relief from "too-much" email, from "inappropriate" email, and from poorly targeted e-mail. Industry, advocates, and governments have reacted by proposing tools or regimes to eliminate spam. Some have proposed placing a price tag on email transmission to deter the sending of large volumes of unwanted e-mail [1]. Lost in all the noise is the idea that e-mail can be an excellent way to start and develop relationships on the internet. Business leaders seek privacy sensitive ways for email to help build relationships as part of the marketing mix.

E-mail marketing can be a great way to efficiently reach customers and prospects. In the optimal e-world individual preferences and interests are shared between groups allowing marketing efforts to be coordinated into sophisticated planned messaging strategies. Practically speaking continued cooperation between marketing groups is difficult to achieve. Companies have a political dimension and its not surprising that there is competition to 'control' the e-mail address and a reluctance to share customer knowledge internally. Brands, Divisions, even in-country Company organizations want to control their customer set and resist passing control, or even knowledge, of their customer to others. Another method must be sought. In IBM's case it's the Global E-mail Cleansing Service (GECS).

We believe that e-mail can be an effective tool for business and customer relationship management. We believe that both business and consumers benefit when e-mail is used effectively in relationship development and management [2]. We believe that consumers, who are willing to accept e-mail, would appreciate highly targeted and relevant messages. We believe that consumers should be able to express their opt-out preferences and have those expressions honored.

This document describes IBM's approach to managing opt-out preferences. We believe that the approach taken by IBM, using GECS as its centerpiece, is a unique and highly effective customer centric approach.

2 Limits of Existing Tools

There have been few attempts, beyond normal marketing database tools, to build applications where consumers can express their opt-out directives. Existing tools encompass the normal 'do not e-mail' codes that most platforms are capable of capturing. Marketers can be trained to select net of these 'do not e-mail codes' and to honor customer opt-outs in this way. Once those codes are in place, it's fairly easy for a database manager to create a list of individuals who do not want e-mail and to send that list to third party list owners for suppression when they sell names to the company or generate marketing messages on behalf of the company.

By way of background, the marketing list business is comprised of four participants: The List Owner, the List Manager, The List Broker and the List User. The Manager represents the owner and sells the owner's lists. The Broker finds lists for the user. List Owners can be list users. In a company, divisions/brands often act as owners.

The situation is more complex when renting lists from third party list providers. The marketer does not want to provide the list provider with their suppression list and potentially compromise the privacy of the individuals on their suppression list. There is no guarantee that the suppression lists sent to a third-party list provider will not be used by that provider to add to their own or other company's marketing lists! Individual marketing campaigns can include many individual lists and without a central suppression processing facility the marketer might have to send individual copies of the suppression list to each list owner and trust them to eliminate the records. The idea of putting dozens, maybe hundreds, of copies of a company's suppression list into the list industry is frightening. Even the FTC is hesitant to suggest that an FTC sponsored Do-Not-Email list could be safely distributed. List owner's have similar concerns about sending their list to individual marketers for processing into their marketing messages.

All parties in the basic infrastructure are scared of sharing their individual lists yet feel that they have to find a way to comply with CAN-SPAM and honor suppression directives. Everyone fears theft of data, misuse and loss of control yet all want to protect the privacy of their customer base.

IBM has first-hand knowledge of suppression lists being inadvertently misused when sent into list owner environments. The long term viability of opt-out management that is dependent on sending suppression lists to every supplier for every order is very poor. To cope with that complexity the middle men (List Brokers/List Managers) in the information sales chain have, in some cases, begun to offer 'suppression list maintenance services'. In these the list brokers/list managers have offered to manage a business' customer suppression list on behalf of the business. While these middle-men are often more trusted then many list owners the volume of suppression systems increases complexity and, in most cases, results in the list owner receiving the suppression list anyway! It also creates an environment where more copies of a company's suppression lists are exposed.

Besides the difficulty of maintaining corporate opt-out lists, large businesses must address a host of internal challenges that make even the maintenance of suppression lists a difficult prospect with existing tools. Larger businesses tend to have several suppression databases and several bulk e-mail applications distributed throughout their organization. When sales forces in multiple divisions, each with their own customer relationship management tools, are added to the mix the situation quickly becomes untenable. Large businesses basically have three choices:

- All data and preferences can be consolidated into a single database with a single control structure.
- When a preference is expressed and recorded in one database, it is immediately communicated, and accepted by all other databases. This is applicable only if the company has a consistent brand identity and honors preferences across all divisions.
- Provide separate privacy statements for each different application so that they can operate independently. This is only acceptable if consumers think of the separate constituencies within an organization as separate entities. It also raises issues regarding when a company share data between entities.

All three of these approaches fall short. Consolidation is an admirable goal but it cannot be achieved over night. While a consolidated database and management environment provides the best approach, it is often not practical. Most complex enterprises have many databases, often in different geographies. Customers can engage with many divisions and each may create records in several of databases. Consolidation of multiple applications and databases in is often not possible in a dynamic environment where individual divisions have differing needs.

To implement the second option, a process has to be created where opt-out information received is sent to all other databases within an organization. However the same privacy concerns that arise when dealing with third-party list brokers can arise within a company with multiple privacy domains. Application owners and marketing group leaders may be reluctant to share their suppression lists with other divisions for fear that they may be misused and hurt their relationship with individual clients. The idea that a customer record might exist in more than one customer database begs the question: 'Whose customer is it?" Honoring a customer's instruction to opt-out of UCE must not be contingent on a company resolving its internal political conflicts.

Separate privacy statements, and separate relationships for each brand handily solves the 'technical' issue but it precludes the free sharing of data across the enterprise. As a business integrates its operation or tries to serve the 'total customer environment' it might well find that it has compromised its ability to serve the customer through potentially conflicting promises in the privacy statement or conflicted instructions from the customer depending on the division/brand the individual was interacting with.. Never-the-less the third possibility is the most viable of the three from a business perspective.

3 Protecting the Customer

IBM is a complex enterprise with a global presence and identity. An individual logging onto an IBM website might easily find they are interacting with a site outside their home country. An individual can browse products outside the scope of their existing business relationship. How does a company like IBM fulfill customer expectations that their information will be used in a manner that recognizes its importance? More importantly how does a company like IBM enable a customer to exert some continuing control over the use of their personal information across the enterprise. When a person's information might reside on the database for more than one division, or in more than one country, how is a person's instruction maintained and honored?

An individual can have a variety of relationships with a company. The more complex the company, the more complex the relationships. Some possible relationships include direct contact resulting from an ongoing engagement, customer services interactions, subscriptions to company newsletters or to specific information products, and transactional correspondence such as bills, shipping notices, and warranty renewals. Of course, they may have no relationship with the company at all and be a total prospect or, as a customer of one brand, they might be a prospect for other brands.

From a Business perspective there is no benefit to antagonizing existing customers. Upsetting customers can only eliminate future information flows and hurt business. Finding a way to capture and honor an individual's opt-out instructions is important to ensuring that the individual welcomes information that they have asked for and greets, positively, ongoing calls from the sales representatives or other personnel that service their relationship. IBM has invested significant energy and resources to develop an application and associated processes to do just that.

The global scale of large enterprises raises additional problems. A customer asking to opt-out may expect that the unsolicited commercial e-mail stop from the company. Yet they may have interacted with multiple databases in multiple countries. The ideal solution must transmit suppression data across the business. Since there is no requirement that databases send their opt-in records to other databases a customer exists in more than one database as the result of their action. Generally, the rules that govern marketing to an existing customer are those in effect in the database where the customer's record exists.

This paper does not tackle the gathering and use of customer 'interests' for targeting. The challenge of gathering customer interests is best handled in the marketing databases using survey or other methodologies. Combining suppression/permission with interest code generation creates additional complexity by combining marketing tactic generation with suppression administration.

4 IBM's Approach

IBM has developed an application and related processes to deliver on its privacy promises and to minimize the perception that it is sending 'spam' to its customers and other constituencies. IBM ensures that the customer, at the point of capture of personally identifiable information, can know about its information practices, is presented with their choices about the use of that data and is given the opportunity to, in most cases, interact anonymously. The databases that support IBM's applications capture and store the codes that result from customer choices.

Another important element is the continuing presentation of opt-out opportunities. All outbound marketing e-mail messages contain instructions that allow the recipient to opt-out of ALL unsolicited commercial e-mail messages from IBM. Newsletters and subscription products carry their own ''unsubscribe' instructions. Since individuals are continually being presented with Notice and Choice and given the opportunity to update their permission in the course of normal business many their instruction from YES to NO and, back again. Some interact more than others but the point is a "NO" is not forever.

IBM targeting personnel are trained to select their marketing lists net of records that have opted-out. This is the first line of customer protection. A customer responding to an e-mail with a 'no more UCE' instruction has that value coded in the sending database first. This is the most likely place for the next commercial e-mail to originate and the immediate encoding of the opt-out instruction in the sending database provides some immediate protection.

The second level of protection is the Global E-mail Cleansing Service (GECS) which tackles the challenge of communicating an individual's instruction across the enterprise. IBM developed and implemented GECS with Harte-Hanks, a global information processor. GECS enables individuals to communicate and change their opt-out value to IBM and have that value communicated to other databases across the enterprise that contain that e-mail address. Synchronization to GECS ensures that other data repositories receive opt-out information in a timely manner. GECS functions in a way to minimize political conflicts between groups so the customer is protected and does not suffer as the result of any inter-divisional conflicts or rivalries. IBM anticipates that, until all databases are consolidated into a single environment, GECS will be a valuable part of its Privacy Management System. The balance of this paper describes GECS and its implementation within IBM.

5 Global Email Cleansing System (GECS)

GECS was conceived in 1999 while the *IBM Guidelines for Processing Business Personal Information* and the *IBM Commercial E-mail Guidelines* were being developed. These incorporated a policy that Notice and Choice would be presented wherever Personally Identifiable Information was gathered. It also required that: *"All marketing or other commercial e-mail, including newsletters, must include a sentence setting forth a simple procedure that a recipient can follow to let IBM know that he or she does not want to receive future marketing or other commercial e-mail from IBM."*[3] An individual following this opt-out procedure expects IBM to stop all future marketing related correspondence. To meet customer expectations, IBM's guidelines further require: *"Before sending a marketing or other commercial e-mail, the IBM employee or agent must screen the prospective recipient against IBM's own suppression lists and, if sending to recipients whose e-mail addresses have been obtained from third party lists, other suppression lists that are recognized and required by IBM."*[4] This required the creation of a database and the incorporation of that database into IBM Processes to assure the individual of a high level of protection. GECS was developed to meet this need. GECS was developed with the following design principles:

1. An individual can say "Yes you may send me unsolicited commercial e-mail" or "No you may not send me unsolicited commercial e-mail". Or they may leave the question unanswered. The Yes or No values are the only two that are proactively provided by an individual.
2. Third parties providing personal information to IBM should be able to screen their lists against the suppression list before providing data to IBM without fear that that data might be moved into the IBM environment. The application was developed at a trusted third party (Harte Hanks) and is accessed via their web site (http://www.messagingcontrol.com). The GECS database does not maintain a record of lists submitted for cleansing nor does it provide any lists submitted to IBM.
3. GECS is neither an e-mail sending engine nor a corporate governance tool. It is 'politically' neutral.
4. The database must function worldwide and adapt to new databases. It was implemented in Brussels to address concerns about transferring European Union data out of the Union.
5. Individuals can change their permission values and be able to start or stop UCE as they desire.
6. Individuals can interact, on the web, with an IBM site anywhere in the world. Opt out requests must be honored world wide.

Traditional approaches to email cleansing often include one or more of the following:

- The creation of a single database with all data,
- The creation of a single e-mail sending engine with a suppression file,
- The simultaneous transmission of opt-out values from one database to all databases with the resulting synchronization/prioritization problems.
- The creation of a single messaging authority to control all e-mail

IBM took another approach by developing a single, simple application that exists for the sole purpose of honoring an individual's opt-out or opt-in requests. This single goal focus meant that it is not bound to the limits of customer data systems and could concentrate solely on the management of customer opt-outs.

GECS receives suppression data from marketing databases in all geographies IBM serves. Additionally sales reps and other customer contact personnel are trained to capture and record customer opt-outs. GECS links to the

Direct Marketing Association's Do-Not-Email list and can link to other 'recognized' suppression sources as required.

The design of GECS is relatively straightforward. However, we still faced a challenge in integrating GECS into our marketing and operational processes in order to take advantage of the protection it affords. Any internal IBM marketer or agent sending unsolicited commercial e-mail to an IBM customer or prospect must either screen against GECS or select from a database that is currently in synch with GECS. GECS screening is not required when an IBM marketer is responding to a customer request (e.g. a subscription) or is in correspondence as part of a transaction or relationship. GECS is a mandatory part of IBM's e-marketing process.

Figure 1. displays the GECS screening process. The GECS screening process works as follows. A marketer uploads their e-mail list via the Harte Hanks website. GECS checks incoming e-mail addresses for structural validity. E-mail addresses with non-valid formats are returned with a 'rejected' indicator so the submitting database can correct their records. Rejected records might contain delimiters (commas or quotes for instance) or might be incorrectly formatted. GECS removes any suppressed e-mail addresses from the list and then sends the list to a protected ftp site with the suppressed e-mails removed. The marketer is notified by e-mail that the list is ready to be picked up from the GECS ftp site. The transaction completes when the marketer picks up the cleansed list and the list of purged e-mail addresses from the GECS ftp server.

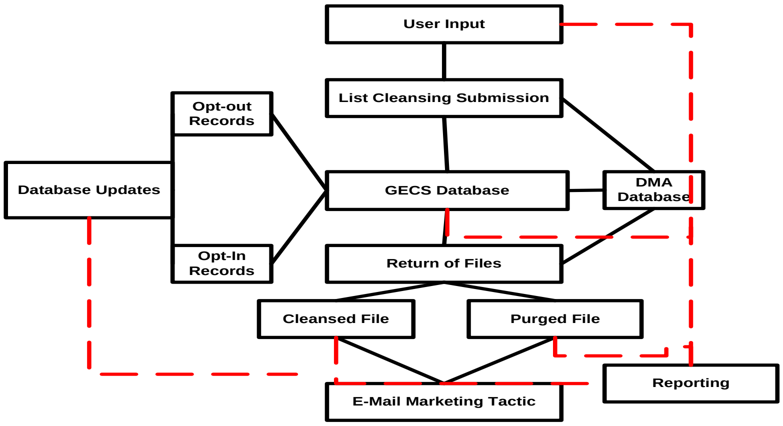


Figure 1. The GECS screening process for comparing marketing lists against suppression databases.

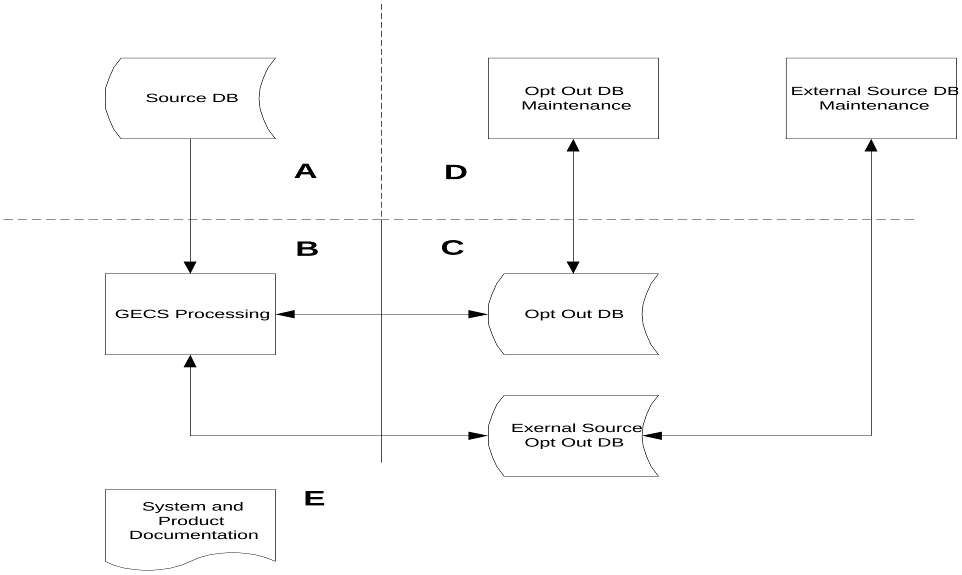

Source DB
Opt Out DB Maintenance
External Source DB Maintenance
A
D
B
C
GECS Processing
Opt Out DB
Exernal Source Opt Out DB
System and Product Documentation
E

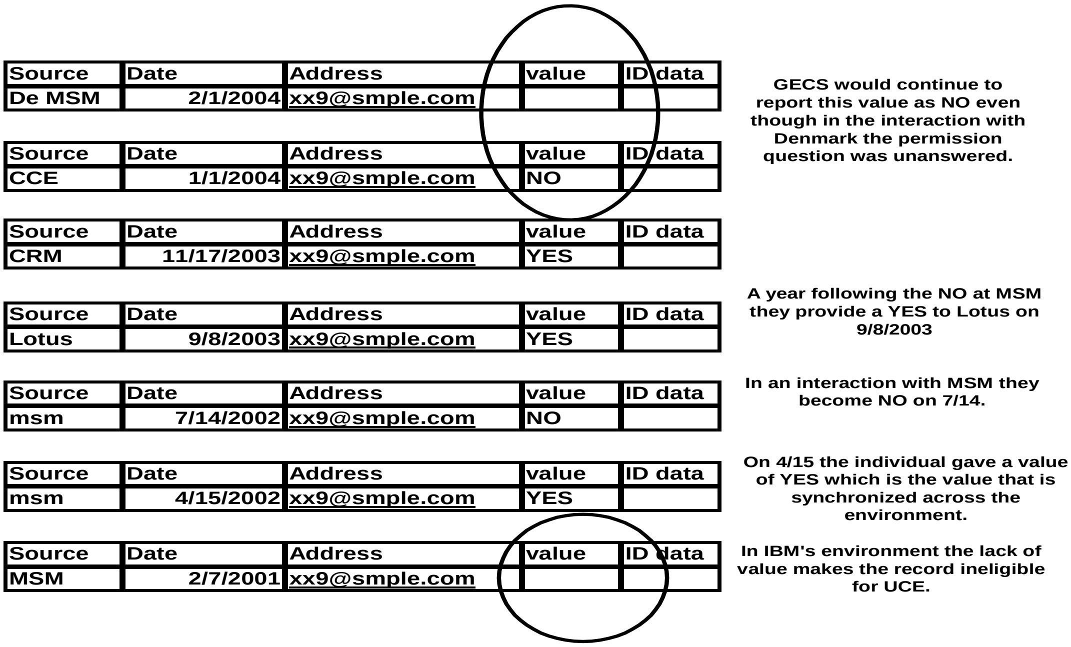
Figure 2. System Architecture of GECS.

6 System Architecture

Figure 2 presents the five basic components of GECS overall architecture:

A. Source list to be cleansed. Generally a flat file in a defined format.
B. Processing engine includes logic, input/output processing, service levels, and exception reporting.
C. Repositories of opt-out information. These may be company proprietary or market standards.
D. Touch points or information gathering applications where suppression information is captured and maintained. Generally these are user applications.
E. System and product documentation includes: service standards, operational procedures, troubleshooting requirements and user help information. Life cycle management and change control is included in this component.

Each interaction IBM has with an individual where an opt-out is recorded is captured in GECS. GECS retains only the information needed to fulfill its mission: e-mail address, suppression date, value, reason code, and source identification. GECS stacks these records taking the most recent customer supplied value (YES or NO) and rippling it across the enterprise. The non-customer supplied value, 'UNANSWERED' or BLANK, never replaces a YES or NO. This logic is reflective of IBM's privacy practices. Table 1 shows several examples illustrating GECS internal logic. IBM presents a consistent Notice and Choice across all groups and its opt-out encompasses all of IBM. The example records shown in the table represent interactions happening in various databases and countries over time. They illustrate that as permission changes the rules associated with the record change and those rules apply across the enterprise.



Source	Date	Address	value	ID data
De MSM	2/1/2004	xx9@smple.com		

Source	Date	Address	value	ID data
CCE	1/1/2004	xx9@smple.com	NO	

GECS would continue to report this value as NO even though in the interaction with Denmark the permission question was unanswered.

Source	Date	Address	value	ID data
CRM	11/17/2003	xx9@smple.com	YES	

Source	Date	Address	value	ID data
Lotus	9/8/2003	xx9@smple.com	YES	

A year following the NO at MSM they provide a YES to Lotus on 9/8/2003

Source	Date	Address	value	ID data
msm	7/14/2002	xx9@smple.com	NO	

In an interaction with MSM they become NO on 7/14.

Source	Date	Address	value	ID data
msm	4/15/2002	xx9@smple.com	YES	

On 4/15 the individual gave a value of YES which is the value that is synchronized across the environment.

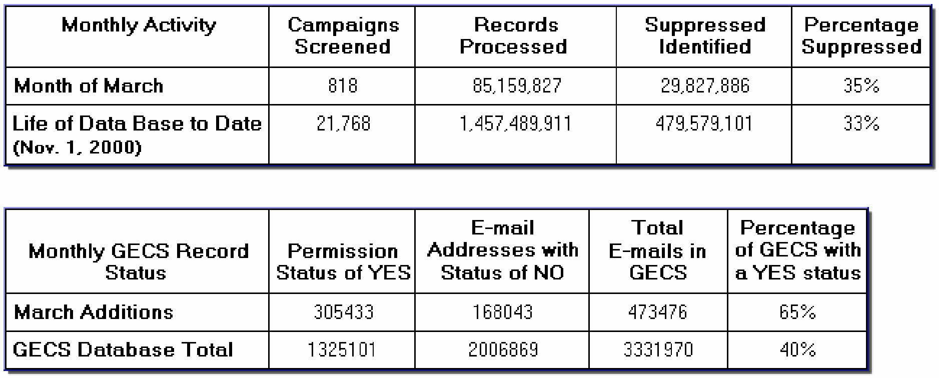
Source	Date	Address	value	ID data
MSM	2/7/2001	xx9@smple.com		

In IBM's environment the lack of value makes the record ineligible for UCE.

Table 1: Sample GECS fields illustrating the logic used to ensure customer privacy.

Marketing Databases are synchronized, on a regular basis, with GECS. The synchronization process is fairly simple. The E-mail addresses (with their values and the date that value was recorded) are submitted to GECS. Each address is checked against the GECS database. Where a match is found the values and dates are compared. The most recent value is recorded, or left, in GECS and returned to the database. An update process encodes the most current 'customer provided' value in the sending database. In this manner the overall e-mail address inventory is kept current. The synchronization process enables IBM to honor a customer opt-out very quickly

Tables 2 and 3 provide some summary statistics about GECS usage. Opt-in addresses are former Opt-outs who have changed status. Folks change from No to Yes in significant volumes. This illustrates that individuals, given the chance to express their preferences may feel more comfortable providing permission back. GECS demonstrates the importance of allowing, in any such system, for individuals to change their values from NO to YES and back again!



Monthly Activity	Campaigns Screened	Records Processed	Suppressed Identified	Percentage Suppressed
Month of March	818	85,159,827	29,827,886	35%
Life of Data Base to Date (Nov. 1, 2000)	21,768	1,457,489,911	479,579,101	33%

Monthly GECS Record Status	Permission Status of YES	E-mail Addresses with Status of NO	Total E-mails in GECS	Percentage of GECS with a YES status
March Additions	305433	168043	473476	65%
GECS Database Total	1325101	2006869	3331970	40%

Table 2: Sample GECS monthly status reports.

Table 3 demonstrates the volume and speed of GECS. Serving a single purpose, honoring customer preferences, simplifies the match and decision logic enough to enable remarkable turnaround times.

Average List Processing Time (minutes)	<5
Average processing time per 1,000 e-mail addresses (seconds)	5.05
Number of Users that have submitted lists	338
Number of Lists Cleansed	18,024
Number of Emails Addresses Cleansed	1,044,642,512
Total Number of Unique Email Addresses in Database	2,738,278
Number of Unique Opt-Out Emails in Database	1,795,753
Number of Unique Opt-In Emails In Database	942,525

Table 3: Statistics of GECS clensing operations since inception.

The process itself is designed to minimize the opportunity for marketing teams to use GECS as a means to protect their own customer set. The returned file does not contain individual list source identification and the entire GECS database is never downloaded to an individual database. Teams cannot place data sets in GECS to reach in and control others while ignoring those entries themselves. Of course, audit records are maintained so the history of individual records can be evaluated if required.

7. Conclusions

Managing customer opt-outs is the responsibility of the Business. Ensuring that customers and non-customers can comfortably transact business, can have a voice in their incoming e-mail load, and can express an opt-out and see it take effect is a substantial undertaking. Anti-spam filtering technologies are “impositional” in nature - they impose regulations and controls from outside any existing relationship. The Global E-mail Cleansing Service (GECS) is a relationship oriented tool built with the customer as its focus. It works within the relationship.

GECS has become a key component in IBM’s overall privacy strategy by ensuring compliance with IBM’s customer “opt-in/opt-out” policy and delivers a unique combination of capabilities in support of IBM’s customer relationships. GECS is but one element of a comprehensive privacy strategy that would be required to ensure an enterprise is meeting its privacy obligations and its objectives for achieving customer trust and loyalty. However, it is an important element and one that is a highly visible indication to customers and the marketplace that the enterprise has a plan and is tackling the issue.

References

1. Saul Hansell, Gates Backs E-Mail Stamp in War on Spam, *New York Times*, February 2, 2004
2. E-mail Can Be Powerful Customer Relationship Tool, *Mortgage Servicing News*, February 2003.
3. *IBM Guidelines for the Processing of Business Personal Information*, IBM, May 15, 2000.
4. *IBM Commercial E-mail Guidelines,* IBM, May 15, 2000.
5. Saul Hansell, Marketers Adjust as Spam Clogs the Arteries of E-Commerce. New York Times, December 1, 2003.
6. David F. Carr, Spam Filtering, The False Positive, *Baseline Magazine,* December 2003.
7. Deborah Fallows. Spam, How it is hurting Email and Degrading Life on the Internet. *Pew Internet & American Life Project*, October 22, 2003.
8. Godwin J. Udo. Privacy and security concerns as major barriers for e commerce: A survey study. *Information Management & Computer Security*, 2001
9. C. Dwork and M. Naor, “Pricing via Processing or Combating Junk Mail”, Lecture Notes in Computer Science 740 (CRYPTO'92), pp. 137-147, 1993.
10. M. Abadi, A. Birrell, M. Burrows, F. Dabek, and T. Wobber. "Bankable Postage for Network Services", *Proceedings of the 8th Asian Computing Science Conference,* Mumbai, India, December 2003.