Whitepaper on a Proposed Do Not Email Registry

April 12, 2004

Issued by: **The Email Service Provider Coalition**
The Interactive Advertising Bureau
TRUSTe

Summary

Email is indeed the “killer app”. In almost every communications context, email has added utility, speed and efficiency. As a society, we have come to depend heavily upon email to transact business, correspond with each other, share information, and market products and services. But the continued success of email is gravely threatened by spam. Unsolicited, fraudulent, deceptive and misleading messages are clogging the email infrastructure and recipients’ inboxes. Put simply, the spam problem will critically damage the interactive industry if it is not curtailed.

For this reason, the Email Service Provider Coalition (ESPC), the Interactive Advertising Bureau (IAB), and TRUSTe – three leading organizations in the interactive marketplace – have joined together to help promote workable solutions to the spam problem. Through a combined membership of over 1500 leading interactive and online companies, the ESPC, IAB and TRUSTe offer a unique perspective into the legitimate use of email and the scourge of spam.

Unfortunately, many of the solutions currently being proposed or used in the marketplace to combat spam are either ineffective or worse damaging to legitimate uses of email. The proposed Do Not Email Registry falls squarely into this category. A Do Not Email Registry would do little or nothing to reduce spam and would, at the same time, layer enormous burdens on the legitimate use of email for marketing purposes.

Jupiter Research estimates that the email marketing industry will grow in size to 8.2 *billion dollars* in 2007. Clearly, this is a sizable and important industry. The size and importance of email in the marketplace should not be measured by dollars alone. Over the past ten years, email has been a strong driver of productivity and efficiency in the marketplace. It has also been an important social tool. Email has shortened distances in the world – allowing communication to occur with unprecedented speed and detail.

As an example of the importance of email, a recent study by the META Group showed that, given a choice between email or telephones, 74% of business people would give up their phones before email. In other words, 74% of people now find email to be more critical than the telephone in their daily work.

These facts point to the critical importance of email in today's world. The ESPC, IAB and TRUSTe have worked extensively over the past 18 months to ensure that the problem of spam does not threaten the utility of email. And just as importantly, the ESPC, IAB and TRUSTe have worked to ensure that solutions to spam do not "throw the baby out with the bathwater" and damage the very thing that we are all trying to protect: legitimate email.

A Do Not Email Registry is Not the Answer

Under the CAN-SPAM Act, the FTC is required to report to Congress setting forth a plan and timetable for establishing a nationwide marketing Do Not E-mail Registry. Given the recent successful implementation of the national Do Not Call Registry for telemarketing, a parallel to email – a Do Not Email Registry -- seems intuitively to make a great deal of sense. Absent a deeper understanding of the technologies, economics and business models involved, one could easily become convinced that a DNE Registry could be an effective solution to the spam problem.

Unfortunately, nothing could be further from the truth. A DNE Registry is a solution that, at best, would be ignored by spammers. At worst, a DNE Registry could cost the marketplace billions of dollars and expose vast numbers of email addresses to more spam. Put simply, a DNE Registry would be ineffective in reducing the amount of spam in consumers' inboxes. At the same time the Registry would impede the growth of e-commerce, confuse consumers, and provide a rich source of valid email addresses for spammers and hackers to target.

The ESPC, IAB and TRUSTe are all opposed to the creation of a DNE Registry. Yet we remain committed to finding workable solutions to reducing spam. Promising technology efforts are underway to address the inherent lack of accountability that exists in email transmission protocols. Legitimate email marketers are coming together to create best practices that respect the informed consent of consumers. And consumers are becoming increasingly savvy about the use of email and methods to prevent spam. All of these efforts would become confused or complicated by the creation of a DNE Registry. These solutions are all showing great promise and should be allowed to succeed before a well-intentioned, but ineffective DNE Registry is mandated.

The DNE Registry is Technologically Problematic

1. SMTP allows for "spoofing" and presents enforcement challenges to a DNE Registry.

Email is delivered through a protocol called the Simple Mail Transfer Protocol (SMTP). SMTP is indeed a "simple" protocol. It was initially developed in a world without spam and, perhaps as a result, lacks many of the tools necessary to ensure accountability within the system.

SMTP allows the sender of an email to obscure his identity as the message is sent. Further use of open relays (email servers that relay email from any sender) and other technologies allows a sender to hide a true identity completely from the ultimate recipient of the message. This lack of identity in the SMTP system allows spammers to send email with relative impunity. SMTP also already presents an enormous challenge with enforcement of the CAN-SPAM Act, and would only increase under any DNE Registry – for enforcement agencies cannot hold unknown senders accountable. It is indeed true that spammers enjoy the impunity of anonymity.

Spammers seek anonymity to avoid accountability for their practices. The stock and trade of a spammer is a constant search for bandwidth through which to deliver their spam and mechanisms that allow them to hide their true identity. SMTP, through the lack of authenticated identity within the technology, allows this abuse to occur.

Most businesses do not fear accountability. As a result, they do not use the tricks used by spammers to obscure their identities within email. Businesses using email for legitimate purposes generally send email from identifiable email servers with IP addresses (the Internet address assigned to the server) that remain static. If a legitimate business sends a message in violation of the CAN-SPAM Act, they can quite easily be identified.

The lack of identity (and therefore, accountability) in SMTP presents a daunting challenge to the effectiveness of any DNE Registry. If created, the FTC would be presented with countless violations of the Registry, but would face the near impossible task of identifying the violators (spammers). The expectations of consumers would assuredly not be met as registrations to the DNE Registry would not materially reduce the amount of spam received by registrants.

2. *The technology required for a DNE Registry would be prohibitively expensive.*

One of the largest challenges associated with a DNE Registry is the sheer volume of transactions that would need to occur in order to screen email campaigns against the list. The technological infrastructure costs to support the millions of requests for access to the list would be daunting – and would potentially run into hundreds of millions of dollars.

There are thousands of organizations that use email on a daily basis. ESPC members provide email delivery services to 250,000 senders within the United States. It is reasonable to assume that each of these senders would need to access the DNE Registry on a regular basis to suppress registered addresses from their lists (daily access would probably be necessary).

Again in contrast to telemarketing, consumers generally have more than two email addresses. And each member of a household is likely to have multiple email addresses – meaning that every household could have numerous email addresses (whereas most households have less than two phone numbers). It is reasonable to assume that the DNE Registry would quickly grow to twice or three times the size of the Do Not Call Registry – meaning that between 100 and 150 million email addresses could be added to the Registry in short order. The size of the Registry would be multiplied over time as email addresses are frequently discarded as consumers move jobs, change ISPs, or simply change their email address. Even more so, ISP's and business often 'recycle' old email addresses to new users, which could further degrade the effectiveness of the registry. It is possible that the Registry could grow to over 500 million email addresses within two years if proper maintenance was not performed on the list.

The processing demands associated with over 250,000 senders accessing a Registry that contains between 100 and 150 million email addresses are prohibitively enormous. The cost for the systems required to support such processing is too expensive to justify the benefit. And it should be noted that these costs would be borne heavily by the organizations that need to access the Registry – for they, too, would need to add capacity to support the processing necessary to cleanse lists.

3. The Registry Would Represent a Single Point of Failure for Email

If a Registry were created, it would present an unacceptable single point of failure to the legitimate businesses that would need to rely on the system. Put simply, the use of a centralized Registry would result in every email marketer being reliant upon the continued functionality of the Registry. Any downtime in the Registry (and such downtime must be expected) could seriously delay or prevent the delivery of legitimate email messages.

It is possible that the Registry would become a target for attacks by spammers and hackers. There are precedents for such attacks being launched against anti-spam efforts. Last year, many of the anti-spam blacklists were disabled due to attacks against the systems used to maintain and distribute the blacklists. Such attacks can be expected to occur upon a DNE Registry – raising the risk of failure of the Registry system.

4. The Registry Would Present an Unacceptable Security Risk

Of all the technological challenges associated with a Registry, one emerges as the most compelling reason to not create a Registry: security. As discussed above, the Registry would quickly grow to include millions of valid email addresses. Such a list would represent the richest source of “live” email addresses ever created. The temptation to technologically-savvy spammers would be undeniable. The Registry would immediately become one of the most visible and coveted targets for spammers and hackers to infiltrate.

Also discussed above was the fact that the Registry would present a single point of failure in the email system. This reality exists with regards to security as well. A centralized Registry would present a single point of failure for the integrity of the email addresses held within the Registry. A single breach of the Registry's security would expose millions of email addresses to vast quantities of spam. And, once the Registry were breached, the email addresses within the Registry would have no protection and would be freely shared and circulated amongst spammers – resulting in even more spam for the registrants. Once these addresses are in the marketplace, the registry would be immediately deemed ineffective, and potentially every registrant would need to change their email address.

There are encryption tools that could be used to improve the security around a Registry. However, history has shown that the best security is still subject to failure. While it is possible that adequate security could be created to protect the Registry from the risks that exist today, it is not possible to ensure the continued viability of such protections in the future. And the risk of a breach (compromised email addresses for all those who registered) is too high to warrant the creation of a Registry.

5. *Promising Technological Solutions to Spam Are Under Development and Should Be Permitted to Succeed Before a Registry Is Mandated.*

The lack of accountability is a well-recognized problem in email. Many efforts are underway to build authenticated identity into the infrastructure of email technology. As discussed above, spammers enjoy the impunity of anonymity. We could begin to hold spammers accountable for their actions if we could take away anonymity in email (through authenticated identity).

In the past year, there has been significant activity around authenticated email. Microsoft has proposed “Caller ID,” Yahoo has released “Domain Keys,” and AOL is testing “SPF.” All of these solutions involve the authentication of some component of the email being sent. And while still in development, these efforts offer promising hope for solutions to spam and should be permitted to succeed before a DNE Registry is mandated.

The ESPC has been active in the promotion of authenticated email through Project Lumos. This effort is designed to offer a road map that will lead industry towards accountability within email. A whitepaper on Project Lumos is available on the ESPC website (www.espcoalition.org).

In addition, TRUSTe has been involved in the Bonded Sender program, offered by Ironport. This program requires that legitimate senders of email post a bond and commit to best practices in email marketing. Violations of the practices results in a loss of a portion of the posted bond. The Bonded Sender program offers an important tool to increase accountability within the legitimate email marketing industry. And when added to an authenticated email system, we begin to see the contours of a more complete solution to spam.

A DNE Registry Would Not Be Effective in Reducing Spam

1. Spammers Would Not Comply with a DNE Registry.

One of the largest problems associated with a DNE Registry is the simple fact that it would not be effective in reducing spam. We know conclusively that spammers do not take heed when new laws are passed. The 37 state laws previously in place would have been effective if spammers were inclined to comply with legal requirements. The passage of the CAN-SPAM Act provided state AGs and the FTC with important enforcement tools, but spammers still have not heeded the rules governing email.

We should not assume that the creation of a DNE Registry will see any different result. The great majority of spam will continue to be sent from anonymous senders that hide behind open relays and spoofed identities. It should also be noted that many spammers operate from overseas locations, beyond the reach of domestic enforcement. As long as they can obscure their identity and hide offshore, spammers will continue to ignore legal requirements, including a DNE Registry.

If few spammers will abide by a DNE Registry, the amount of spam will not noticeably decrease. And that raises a fundamental question: why create a DNE Registry if it will not result in a decrease in the amount of spam? Clearly, we should not pursue an expensive and security-impaired solution without a very strong indication that it will achieve the desired effect of reducing spam. A DNE Registry fails this test.

2. Spammers Are Already Violating the Law.

In a 2003 study, the FTC found in a random survey of 1000 pieces of spam that fully two thirds of the email reviewed included some indication of falsity.[1] This statistic is borne out by a review of any email inbox: spam is based upon falsity and fraud. Spammers are thus already violating the law. Their messages are presumably in conflict with existing consumer protection standards at both the state and federal levels.

The CAN-SPAM Act adds more tools for enforcement agencies and clarifies that some practices are indeed illegal (such as harvesting email addresses, creating

[1] “False Claims in Spam,” A Report by the FTC’s Division of Marketing Practices, April 30, 2003.

multiple email accounts for purposes of spamming, or falsifying header information). Yet spammers continue to ignore these standards.

We cannot assume that spammers will comply with a DNE Registry. Indeed, we should assume that they will not. Spammers are already violating the law and will continue to do so under a mandated DNE Registry.

The creation of a DNE Registry will divert resources from important enforcement actions under the FTC Act and the CAN-SPAM Act. These existing laws should be enforced vigorously and allowed to achieve the full measure of their intended purpose before a DNE Registry is considered.

3. Legitimate Email Marketers Are Not Spamming.

The use of email by marketers has proven to be a powerful and effective tool in the marketplace. But abusing the interests of consumers is not effective. Marketers that intend to be in the marketplace over time cannot afford to spam their potential or existing customers. Indeed, the effects of ISP filtering due to consumer complaints can threaten the viability of a marketer if they do not respect consumer concerns in the execution of their email campaigns. Legitimate email marketers have enormous incentives to deliver email that complies with the expectations of the recipient.

Given this reality, the marketplace has responded with best practices that respect the consumer's inbox. Increasingly, legitimate email marketers are delivering messages only to recipients that have provided informed consent to receive email. The ESPC released a "pledge" for members in 2003 (attached as Appendix B) that requires that "unsolicited commercial email shall not be sent." The need for informed consent prior to delivering marketing messages via email has become a business imperative for legitimate companies.

It follows that a DNE Registry is unwarranted if spammers are going to ignore the Registry and legitimate email marketers are obtaining the informed consent of recipients prior to sending email. Again, for what purpose would a Registry be created if those to whom the Registry was targeted would not participate?

A DNE Registry Would Present Enormous Implementation Challenges

1. *Confusion Would Be Created as to What Messages Must Be Screened Through the Registry.*

One of the major differences between telemarketing and email is the breadth and variety of messages transmitted. Telemarketing was exclusively the domain of marketing messages. Email is used to deliver a multitude of messages of every conceivable variety. Newsletters, account statements, personal communications (including one-to-one marketing or advertising), transaction reports, and affinity messages (such as alumni bulletins from a college) are all delivered through email. Many of these messages also contain promotional or advertising material. In some cases, the promotional content is significant and is used to support the primary purpose of the email (*i.e*., newsletters).

Parsing these various communications to determine what would be subject to the Registry would be a daunting and confusing task. A DNE Registry would need to have an exhaustive list of exceptions to cover the messages that consumers expect to receive even after their email address is registered.

2. *The DNE Registry Would Need to Include Volume Triggers, Further Complicating Implementation.*

The CAN-SPAM Act does not include any volume triggers for compliance with the Act. In other words, a single non-compliant email can result in exposure under the Act. While this is a concern under the CAN-SPAM Act generally, volume triggers would be an absolute necessity under a DNE Registry. But tracking volume and ensuring compliance would be a nearly impossible task under a mandated DNE Registry.

Many unsolicited commercial email messages are personal communications. A local real estate agent may send an unsolicited email to a homeowner considering selling their home. Or a branch loan officer may learn that someone in their town is looking for financing and send an email introducing their services. Each of these communications is an unsolicited commercial email message. Yet each message was sent only as a single communication to a single recipient.

The CAN-SPAM Act does not include any exemptions for low-volume or personalized messages. As a result, single emails (as described in the examples above) can create exposure for the organizations sending the messages.

A DNE Registry would need to exempt low-volume or personalized messages. Failure to do so would have catastrophic effects on the free flow of communication at a local and personal level. Large organizations would need to filter all outgoing email communications – including messages sent by local employees to individual prospects – through the DNE Registry. This would delay and burden the growth of email as a powerful communications tool.

3. A DNE Registry Would Disproportionately Harm Small Businesses.

Much commercial email is sent from small businesses. The power and simplicity of email communication has not been lost on the millions of smaller organizations around the country. For most of these organizations, technological resources are limited. Email works for them because it is cost effective, simple, and successful.

Adding a DNE Registry to their obligations would present daunting resource challenges and may result in a migration of small business *away* from email.

As discussed above, the technological challenges of a DNE Registry are overwhelming. Sophisticated security systems and file sharing mechanisms would need to be used to prevent abuse. These same safeguards will present an insurmountable challenge to small businesses with limited technology expertise. Small businesses will not be able to incorporate the required security into their operations in a cost-effective manner. Indeed, small businesses may not be able to support the costs associated with implementing a DNE suppression process, period. This dynamic could have the harmful effect of disproportionately forcing small business away from email as a marketing tool.

Comparisons to the Do Not Call Registry Are Inappropriate

One of the drivers for the inclusion of a DNE Registry study within the CAN-SPAM Act was the tremendous popularity and successful implementation of the FTC's Do Not Call Registry for telemarketing (the "DNC Registry"). It intuitively follows that a DNE Registry would be similarly popular and easily implemented. But such intuition is flatly incorrect. Email differs markedly from telemarketing. An understanding of these differences leads to a clear understanding: a DNE Registry would not work for email marketing.

1. Telemarketers Are Identifiable and Accountable, Spammers Are Not.

As discussed above, spammers send their messages with the impunity of anonymity. Spammers can abuse SMTP to obscure their true identities. As a result, they remain unaccountable for their actions. In contrast, telemarketers are fairly easy to find – they can be tracked by the phone number from which they are calling.

Accountability must be a condition precedent to the creation of a DNE or DNC Registry. We have accountability in telemarketing due to our ability to track phone numbers. We do not have accountability in email due to the ability of spammers to spoof their identities. As a result, a DNE Registry does not allow for effective enforcement, while a DNC Registry can be very effective.

2. The Cost of Creating and Sending a Message Is Very High in Telemarketing and Very Low in Email.

To engage in telemarketing, telemarketers must invest heavily in the actual transmission costs of their messages (the toll for the phone call). They must also pay for the human resources to actually make the calls. Again in contrast, the costs to create and deliver an email message are very low. A spammer can send millions of messages with negligible technological and human costs.

As a result, telemarketers have a compelling incentive not to call those individuals who do not wish to receive calls. It simply costs too much to make a call that has no chance of success. In contrast, spammers have every incentive to ignore the interests of recipients. For a spammer, volume does not increase costs dramatically. In fact, for a spammer, volume is critical – as the response rates to spam are infinitesimally low.

Thus, a DNC Registry works for the telemarketing industry – telemarketers have a strong economic incentive not to send messages to people on the DNC Registry. But a DNE Registry would prove ineffective in stopping spammers, as they have no economic incentive to reduce the volume of their messages.

3. Vast Public Records of Telephone Numbers Currently Exist, Similar Email Records Do Not.

The majority of personal telephone numbers in the United States are available through public directories (phone books). As a result, it is fairly easy to find the listed phone number for any person in the country. The cost of creating and transmitting a phone call helps to prevent the abuse of these public listings.

In contrast, email addresses are not included on any master directories. An email address is, currently, a private identifier that is disclosed at the discretion of the owner. This system is logical given the abuse that would occur if a large directory of email addresses were created. The comparative lack of economic inhibitors to volume email would see spammers immediately abusing such directories if they were to be created.

The creation of a DNE Registry raises unanswered concerns about aggregating vast numbers of email addresses in a single location. We simply cannot afford the risk of abuse of such a list where the cost of sending millions of email messages is so low. A DNC Registry presents no additional risk to the numbers listed in the DNC Registry (they are already available publicly already). A DNE Registry presents enormous risks to the email addresses listed in the DNE Registry, as no such directory otherwise exists.

Conclusion

A Do Not Email Registry is intuitively a compelling tool to reduce spam. But the reality is that a DNE Registry will create far more problems than it actually solves. The costs to business and the public to build the infrastructure necessary to support the sheer volume of transactions through a Registry will be staggering. The potential security exposure associated with the world’s largest directory of email addresses is simply too risky to condone. And most importantly, a DNE Registry will do nothing to deter spammers! Consumers registering to the list will not notice a decrease in spam and may, in the event of a security breach, see much, much more junk email in their inboxes.

There is significant work being done in the marketplace today to respond to spam. Legitimate businesses are defining best practices that respect the informed consent of consumers. Important studies are showing consumers how to properly safeguard their email addresses to prevent spam. And technology is being developed to bring accountability into the email system. A DNE Registry would take scarce resources away from these important efforts.