IAC/InterActiveCorp

June 27, 2005

Via Electronic Filing

Mr. Donald S. Clark
Secretary
Federal Trade Commission
Room 159-H
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Re: CAN-SPAM Act Rulemaking, Project No. R411008

Dear Secretary Clark:

IAC/InterActiveCorp ("IAC") submits these comments to the Federal Trade Commission ("FTC" or "the Commission") pursuant to the FTC's May 12, 2005 Notice of Proposed Rulemaking ("NPRM") regarding Definitions, Implementation, and Reporting Requirements Under the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM" or "the Act"), 70 Fed. Reg. 25,426 (2005). IAC strongly supports the goals of CAN-SPAM and the Commission's NPRM: curbing the barrage of unsolicited commercial electronic mail and preserving consumer privacy and choice, while maintaining the usefulness and efficiency of electronic mail as a means of communication for legitimate organizations. IAC commends the Commission for its Proposed Rule, which represents a thoughtful and careful effort to achieve that delicate balance between consumer privacy and business flexibility, and appreciates the Commission's thorough consideration of IAC's comments on its March 11, 2004

152 West 57th Street, 42nd Floor, New York, New York 10019 212 314 7300 Fax 212 632 9600

Advance Notice of Proposed Rulemaking ("ANPR"). While IAC believes that the Proposed Rule generally achieves the purposes of the Act while preserving the ability of legitimate businesses to communicate by electronic mail, it respectfully submits these comments to clarify four aspects of the NPRM.

BACKGROUND

As IAC described in its comments on the ANPR, its operating Businesses provide a broad array of products and services to consumers worldwide. IAC's Businesses operate in such areas as travel services (Classic Custom Vacations, Expedia, Hotels.com, Hotwire.com, Interval International, TripAdvisor), electronic retailing (Gifts.com, Home Shopping Network), event ticketing (Ticketmaster), personals and networking (Match.com, uDate, ZeroDegrees), financial services and real estate (Domania, RealEstate.com, LendingTree), and local and media services (Citysearch, Entertainment Publications, Evite, ServiceMagic). Most of these Businesses offer many of their products and services online, and operate full-service websites for their customers, members, subscribers, and visitors.

For IAC's Businesses, electronic mail is an essential tool in facilitating transactions, communicating with customers, and providing relevant additional information to customers and other consumers. For example, an individual who purchased an airline ticket through one of the travel Businesses may receive a follow-up e-mail before his or her travel date with information about the weather conditions in the destination city, as well as about special hotel or rental car offers in that city which he or she may find of interest. Many of the Businesses also send electronic newsletters to their customers or members as an added benefit of using the company's website, and often e-mail their members to update them on special promotions and discounts being offered by

the third parties whose products and services those Businesses feature. In many cases, the ability to receive these follow-up emails, newsletters, and information about special promotions is a primary reason that an individual has become a member or subscriber of an IAC Business. The Businesses also advertise their own products and services by electronic mail in a variety of ways, including by sending an e-mail (either directly or through a list broker) to their own members or customers; by advertising in messages sent by another IAC Business to that Business' members or customers; or by advertising in messages containing advertisements for multiple companies that are sent by third parties to those third parties' own subscribers or members of a mailing list.

ANALYSIS

IAC submits these comments to the Commission on four aspects of its Proposed Rule. First, IAC asks the Commission to clarify that under its proposed definition of "sender," an entity "controls the content" of a message only if it controls the content of the overall message – and not just one or more component parts. Second, IAC supports the Commission's suggestion that the FTC should create a safe harbor to limit the liability of an entity whose products are advertised in messages sent by affiliates or other third parties over whom the entity has no control. In these comments, IAC proposes that entities meeting a four-part compliance test should be covered by this safe harbor. Third, IAC urges the Commission to adopt as part of its Final Rule its proposal that a Post Office Box be deemed a "valid physical postal address" under the Act. Fourth, IAC respectfully requests that the Commission reconsider its proposal to reduce the time for honoring opt-out requests from ten to three business days, a change that is not supported by the underlying record and would burden legitimate businesses without any corresponding benefit to consumers.

I. THE FTC SHOULD CLARIFY THAT AN ENTITY "CONTROLS THE CONTENT" OF A MESSAGE ONLY IF IT HAS AUTHORITY OVER THE CONTENT OF THE ENTIRE MESSAGE.

Under the CAN-SPAM Act, a "sender" of a commercial electronic mail message is defined as "a person who initiates a [commercial electronic mail message] and whose product, service, or Internet web site is advertised or promoted by the message." 15 U.S.C. § 7702(16)(A). The Act requires a sender, among other obligations, to provide a method by which a recipient may opt out of messages from the sender, and to honor subsequent opt-out requests within ten business days. In its Notice of Proposed Rulemaking, the FTC proposes modifying the definition of "sender" such that, when more than one person's products or services are advertised or promoted in a commercial e-mail message:

> each such person who is within the Act's definition will be deemed to be a "sender," except that, if only one such person both is within the Act's definition and meets one or more of the criteria set forth below, only that person will be deemed to be the "sender" of that message:
>
> 1. The person controls the content of such message;
> 2. The person determines the electronic mail addresses to which such message is sent; or
> 3. The person is identified in the "from" line as the sender of the message.

70 Fed. Reg. at 25,451. The proposed definition is intended, in particular, to enable entities to identify and even designate the "sender" of messages promoting the products and services of multiple advertisers. Id. at 25,430.

IAC supports the FTC's proposed definition of "sender" as a way to alleviate the complexity and confusion surrounding commercial e-mail messages that contain material advertising the products and services of multiple entities. The key

compliance challenge of the proposed definition of a "sender," however, will be determining which entity "controls the content" of a commercial message in these instances. IAC asks the FTC to clarify that an entity only "controls the content" of an e-mail message if it has final approval authority over the content of the entire message and is thereby responsible for compiling various components into one overall message. In contrast, simply reviewing the message, providing some of the graphics, or drafting just a portion of the message's text is insufficient to "control the content" of that message.

This reading of "controls the content" is necessary to remain consistent with the Proposed Rule because the opposite interpretation – that any entity which has provided any component of the message's content "controls" it – would defeat the purpose of the three-pronged standard for identifying a single sender. By definition, all of the advertisers whose products are promoted in a message will contribute some content to that message. Accordingly, this minimal level of control cannot be the standard contemplated by the Commission. IAC suggests that, instead, the only logical interpretation is that the entity with final approval authority over the commercial e-mail – which is the entity responsible for compiling the component pieces into a complete message – controls the content of the message under the Proposed Rule.

This approach is consistent with the FTC's rationale for the "controls the content" standard and the definition of "sender" in the Proposed Rule. As IAC noted in its April 2004 comments and as the Commission appears to have recognized in its recent NPRM, "[W]hen consumers have subscribed to an online newsletter or similar service, they would expect to submit an opt-out request to that newsletter publisher, not to each advertiser in the newsletter." 70 Fed. Reg. 25,429-30. Moreover, one of the criteria for

identifying the sender under the Proposed Rule is which entity determines the list of recipient e-mail addresses – and, accordingly, to which a consumer would logically expect that a meaningful opt-out request should flow. Yet if "controls the content" meant that an entity has <u>any</u> influence over <u>any</u> component of a message, all of the advertisers in the newsletter example would be senders. This result would obviate the purpose for the Commission's proposed change to the definition of "sender."[1] The approach is also consistent with Congress' intent in enacting CAN-SPAM. Specifically, Congress imposed additional obligations on the sender of a message – namely, that opt-out requests apply only to the "sender," which is therefore the entity from whose communications a recipient would reasonably expect to unsubscribe.

IAC therefore urges the FTC to clarify that an entity only "controls the content" if it has final approval authority over the entire message and is thereby responsible for aggregating the component parts of the e-mail from different sources into the final message.[2]

---

[1] As the Commission noted, the use of standards based on the consumer's perspective is consistent with "the analytical approach the Commission traditionally has taken with advertising." 70 Fed. Reg. at 25,430.

[2] In its April 2004 comments, IAC asked the Commission to clarify that the transactional/relationship exception extends to messages from all parties to a transaction in which a customer has engaged. IAC sought this clarification because of section 7704(a)(4)(A)(iv) of the Act, which prohibits a sender or any person who knows of a consumer's opt-out request from subsequently sharing that consumer's e-mail address for any purpose other than compliance with law. Under the strict letter of that clause, if a consumer purchased a United Airlines ticket from Expedia, but then opted out of receiving future marketing e-mails from Expedia before Expedia had shared his or her e-mail address with United (or had previously opted out of receiving marketing e-mails from Expedia), the Act would preclude Expedia from disclosing that customer's e-mail address. Thus, absent this clarification, that section of the Act could be interpreted to prohibit companies such as Expedia from disclosing a customer's e-mail address to another party involved in a transaction – even when that party needs the e-mail address to facilitate or complete the transaction.

II. THE FTC SHOULD CREATE A SAFE HARBOR FOR COMMERCIAL MESSAGES SENT BY AFFILIATES OR OTHER THIRD PARTIES OVER WHICH AN ADVERTISER HAS NO CONTROL.

In the NPRM, the Commission declined to exempt entities from liability for e-mail messages advertising their products and services that are sent by affiliates and other third parties over which the advertisers have no control. The Commission did, however, propose the establishment of a safe harbor in this situation so that entities that complied with the provisions of this safe harbor with respect to those affiliates and other third parties would be insulated from liability under the Act, and sought comment on the appropriate criteria for such a safe harbor.

IAC supports the creation of a safe harbor in this context as a means to protect consumers while providing clear guidance and much-needed flexibility to the countless legitimate businesses that rely on affiliates and other third parties as an integral part of their e-commerce activities. IAC believes that the Commission's safe harbor under the Telemarketing Sales Rule ("TSR") is a successful and useful model, although certain key distinctions between the telemarketing and e-mail contexts support the creation of a modified approach with respect to CAN-SPAM. Specifically, IAC recommends that underlying advertisers not be held responsible for e-mail messages promoting their products and services that are sent by affiliates and other third parties if:

1. The advertiser contractually requires the affiliate or third party to comply with CAN-SPAM;

In the NPRM, the Commission suggested that the transactional/relationship exception extends to all parties to a transaction – at least in the Expedia example. See 70 Fed. Reg. at 25,434. IAC appreciates this important clarification. In stating this, however, the NPRM could be construed to suggest that Expedia may not be the sender of subsequent messages relating to that transaction. IAC respectfully requests that the Commission clarify this point. Specifically, in the example cited by the Commission and in general, Expedia should be treated as a sender of any message it transmits that advertises or promotes its services.

2. The advertiser requires the affiliate or third party to certify periodically and in writing that it complies with CAN-SPAM;

3. The advertiser provides the affiliate or third party with written guidelines on how to comply with CAN-SPAM; and

4. The advertiser maintains additional reasonable procedures to ensure that the affiliate or third party complies with CAN-SPAM.

A. The Affiliate Model

The affiliate system is at the core of modern e-commerce.[3] Much more than in the offline world, online entities maintain vast networks of third-party affiliates that they rely on for promotions and referrals. These affiliates are diverse in both nature and size: they range from massive multi-billion dollar retailers and organizations to tiny "mom-and-pop" entities that operate a single website or generate only occasional promotional material. In general, affiliates receive no guidance on how or even whether to promote or market the underlying seller's products. Instead, affiliates are compensated in two ways: (1) for each "click" that they generate, and (2) for each sale that they generate. Thus, an affiliate that includes an Expedia promotion on its website will receive a small fee from Expedia each time a user clicks on the Expedia link and is directed to the Expedia website. If the individual then purchases a product from Expedia, the affiliate will receive an additional fee. Similarly, an affiliate that includes information about Expedia in an electronic newsletter will be paid for each click-through from that newsletter onto the Expedia website, and will be paid additional money for each subsequent purchase of a product or service from Expedia. This commission-driven model pervades online advertising, and it is the key factor that enables most entities –

[3] To be clear, IAC believes that any safe harbor should apply with respect to both affiliates and third-party service providers. We provide additional background on the use of affiliates by Internet companies because of the unique issues raised in this context.

including the IAC Businesses – to offer so many online services and so much online information free of charge to users.

The number of affiliate-based agreements on the Internet is staggering. Expedia, for example, has tens of thousands of affiliates. While many of these affiliates may be dormant, roughly one-quarter of Expedia affiliates generated clicks in 2004; of those, more than one-fifth initiated an Expedia transaction in 2004. Despite the total number of affiliates, however, a minority of these entities generated a significant number of transactions in 2004; thus, just a small percentage of Expedia's affiliates were responsible for the vast majority of sales made through the affiliate program. Nonetheless, the unique nature of the Internet makes the continued existence of a broad affiliate program critical: it enables Expedia to promote its products and services broadly to users that it might not otherwise be able to reach; and it enables small or targeted affiliates to thrive by maintaining limited arrangements with literally thousands of different partners.[4]

There is no offline analog for these affiliate programs. The ability to track online click-throughs and purchase paths is unique to the Internet, and the ease of moving among websites and electronic communications is essential to these affiliate arrangements. Users can click through from e-mails, search engines, or websites to a particular site in order to find more about – and potentially purchase – a product or service of interest to them. Affiliates are paid just a tiny fee for each click-through or

---

[4] Expedia is not alone among the IAC Businesses in its use of such a broad affiliate program. HSN, for example, has several thousand affiliates in a system that operates much like Expedia's, and Entertainment Publications also has several thousand affiliates. Correspondingly, many of the IAC Businesses may be the affiliates of other companies – paid by those companies for each click and transaction just as they compensate their own affiliates.

transaction they generate; this click-based inter-connectivity allows users to take seamless virtual tours, shopping trips, and information-gathering excursions. These affiliate programs are distinct from agreements with other third parties, including commercial list brokers, where those third parties are paid a flat fee to send out a particular commercial e-mail messages (or particular promotional material in a larger e-mail) to a defined set of recipients. That situation is much more analogous to the traditional telemarketing context covered by the TSR safe harbor, where an underlying seller contracts with a unique third-party telemarketer (or a finite and limited set of telemarketers) to promote its products. In those cases, the underlying seller can and should exercise a significant degree of control over the intermediary marketer – because those marketers are limited in number and have been hired to perform a specific task on behalf of the seller. In contrast, many online businesses maintain tens of thousands of online affiliates, and these affiliates are not "hired" to do anything – they are simply paid a small fee for referrals. And unlike list brokers and telemarketers, many affiliates are not even in the marketing business; they may be trade associations, non-profit entities, or other online retailers seeking additional revenue streams.

B. The Safe Harbor

The Commission stated in the NPRM that "it is inappropriate to excuse content providers in advance from the obligation to monitor the activities of the third parties with whom they contract." 70 Fed. Reg. at 25,431. IAC agrees, and it endorses the Commission's specific decision in the telemarketing context to hold "sellers liable for the actions of third-party representatives if those sellers have failed to adequately monitor the activities of such third parties and have neglected to take corrective action when those parties fail to comply with the law" – particularly with respect to do-not-call procedures.

Id. However, the language of CAN-SPAM and the unique context of the Internet, particularly in light of the pervasiveness of per-click affiliate agreements as a means to enable free services on the Web, dictate a safe harbor that is based upon the TSR but tailored to the Internet medium.

In most circumstances, CAN-SPAM does not subject the underlying seller to liability for commercial e-mails transmitted by affiliates. Under the Act, an entity that "initiates" a commercial e-mail message is directly subject to liability under the Act for that message. To "initiate" means "to originate or transmit such message or to procure the origination or transmission of such message"; to "procure," in turn, means "intentionally to pay or provide consideration to, or induce, another person to initiate such a message on one's behalf." 15 U.S.C. §§ 7702(9), (12). As the NPRM notes, to "procure" an e-mail, "one must do something that is designed to encourage or prompt the initiation of a commercial e-mail." 70 Fed. Reg. at 25,441. But, in the affiliate context, the underlying seller usually does not "procure" affiliate e-mail messages; rather, the affiliate is simply paid for a click-through to the seller's site, and is not affirmatively encouraged or even specifically authorized to send promotional e-mail messages. The affiliate instead receives a limited license to use the seller's trademark and advertising material to promote the seller's products and services. The underlying seller may not know that a particular e-mail exists until well after it has been transmitted, and in many cases, may never know of an affiliate-generated e-mail. Under most circumstances, then, CAN-SPAM does not subject the underlying seller to liability for these affiliate e-mails – because any such e-mails are created and transmitted entirely at the discretion of the affiliate.

However, in those situations where an affiliate is encouraged to send a particular e-mail on behalf of the underlying seller, or in other instances where the Commission may find that the seller procured an e-mail transmitted by a third party, a safe harbor is not only appropriate but essential. In particular, the sheer volume of affiliates and the pervasiveness of the affiliate-based system on the Internet simply make it impossible for companies to exercise any meaningful oversight or control with respect to affiliate e-mails.

Such a safe harbor should have four components. First, the advertiser should be required to mandate by contract that the affiliate or third party comply with CAN-SPAM. This contractual component is critical: it explicitly binds the affiliate to the terms of the Act, and it helps protect the underlying seller in the event of potential violations by the affiliate.

Second, the advertiser should be required to have the affiliate or third party certify periodically and in writing that it complies with CAN-SPAM. This certification further binds the affiliate to the requirements of the Act while providing additional protection to the seller. Moreover, the certification constitutes an affirmative act by the affiliate indicating compliance with CAN-SPAM. The frequency of the certification should depend on the circumstances of the seller-affiliate relationship; for example, an affiliate known by the seller to send promotional e-mail routinely should be subject to more frequent certification than an affiliate that is dormant or rarely sends e-mail.

Third, the advertiser should be required to provide the affiliate or third party with written guidelines on how to comply with CAN-SPAM. In contrast with the

safe harbor under the TSR – which requires compliance training, – the CAN-SPAM safe harbor should allow sellers to provide to their affiliates written guidelines on how to comply with the Act. See 16 C.F.R. § 310.4(b)(3)(ii). An advertiser should be permitted to provide these guidelines once – at the time of entering into an agreement with the affiliate – including by means of a web page within the affiliate section of its website. As noted, while a seller will typically contract with only a small number of telemarketers – and will therefore have the resources to affirmatively train those telemarketers on compliance with the TSR – an advertiser often contracts with thousands of affiliates in the online context. Because of the sheer number of affiliates, there simply is no reasonable way that an advertiser can affirmatively train those affiliates on the requirements of CAN-SPAM. The use of written guidelines, however, would serve the same purpose – particularly to the extent that affiliates are required to certify that they have read and understand those guidelines, and that they are taking steps to comply with the Act.

Fourth, the advertiser should be required to maintain additional reasonable procedures to determine whether those affiliates or third parties that are sending commercial e-mail messages are complying with CAN-SPAM. The TSR safe harbor requires a seller to "monitor[] and enforce compliance" with its procedures under the rule. Id. § 310.4(b)(3)(v). Again, this affirmative monitoring obligation is reasonable in the telemarketing context, where sellers can perform random quality control tests of the limited number of telemarketers with which they have contracted for a specific service. But there simply is no way that advertisers can engage in similar practices with respect to affiliates under CAN-SPAM: each advertiser contracts with thousands of affiliates;

generally does not encourage or even specifically authorize an affiliate to send e-mail messages on its behalf; and often does not even know that a particular e-mail message has been sent until after the fact, if at all.

Instead, advertisers should fall within the safe harbor if they implement "reasonable procedures" to determine compliance with the Act.[5] These procedures may include obtaining sample e-mails from those affiliates or third parties that an advertiser learns are sending commercial e-mail messages that advertise its products or services; designating an individual within the advertiser's organization to sign-up for and receive commercial e-mail messages sent from those affiliates or third parties that the advertiser knows are sending commercial messages promoting its products or services; and taking remedial action against those affiliates or third parties that an advertiser learns are sending commercial e-mail messages that violate the Act.

Given the volume and variety of affiliate relationships, no one set of procedures or terminology could comfortably be applied to all possible circumstances. For example, a vendor that an advertiser hires to send e-mail on its behalf or an affiliate that an advertiser learns generates a significant number of click-throughs from commercial e-mail messages will certainly require a different degree and type of

---

[5] A similar standard has been used successfully by federal agencies in analogous contexts; such a standard offers strong protection to consumers while allowing businesses much-needed flexibility. For example, the Federal Reserve Board has held that a failure to obtain written authorization for recurring payments on a debit card does not violate Regulation E "if the failure to obtain written authorization was not intentional and resulted from a bona fide error, and if the payee maintains procedures reasonably adapted to avoid such error." 69 Fed. Reg. 55996, 56003 (Sept. 17, 2004). Similarly, Treasury regulations require money services businesses to take reasonable steps to guard against the flow of illicit funds into the United States from foreign sources. 31 C.F.R. pt. 103, app. C. The "reasonableness" standard is an important feature of each of these rules because it allows each business to tailor its procedures "depend[ing] on a variety of factors specific to each agent or counterparty." Id.

oversight than an affiliate that has generated few or no such click-throughs. Similarly, an affiliate or other third party that prompts complaints of violations will require a different response from the advertiser than an affiliate that has consistently demonstrated impeccable practices. The advertiser should therefore have the flexibility to determine what procedures are reasonable; in contrast, any strict requirement of monitoring or enforcement would impose a tremendous cost and resource burden on these advertisers without any corresponding benefit for consumers.

III. THE FTC SHOULD ADOPT ITS PROPOSAL THAT POST OFFICE BOXES ARE VALID PHYSICAL POSTAL ADDRESSES.

The Proposed Rule confirms that a Post Office Box constitutes a valid physical postal address under the Act. IAC urges the FTC to adopt this proposed change in its final rulemaking. The use of a P.O. box is consistent with the purposes of the physical postal address requirement because it: (a) provides a means by which senders can receive written correspondence, including legal process; (b) requires senders to designate a single physical location for receipt of such correspondence; and (c) allows the FTC and other government agencies to confirm the physical location and identity of senders.

As IAC explained in its comments on the ANPR, the use of P.O. Boxes as physical postal addresses also ensures that businesses can protect themselves against the growing threats to their security. IAC Businesses, like many large organizations, store vast amounts of personal information concerning consumers and employees, making them attractive targets for criminals and terrorists intent on causing physical or economic harm to the Business, its customers, or the national economy. IAC Businesses use sophisticated techniques to protect the security of their offices and personal data, but it is

never possible to completely eliminate such threats. The use of a Post Office Box in an electronic mail message instead of a street address is one important method of discouraging criminal activity against businesses and their customers. The Final Rule should therefore adopt the FTC's proposal that a Post Office Box is a "physical postal address" under CAN-SPAM.

IV. THE FTC SHOULD NOT REDUCE THE TIMEFRAME FOR HONORING OPT-OUTS TO THREE BUSINESS DAYS.

CAN-SPAM gives the Commission authority to modify the statutory ten-business-day timeframe for honoring opt-out requests if it finds that an alternative timeframe "would be more reasonable after taking into account the purposes [of the Act's opt-out provisions]; the interests of recipients of commercial electronic mail; and the burdens imposed on senders of lawful commercial electronic mail." 15 U.S.C. § 7704(c). To reduce the statutory timeframe, the FTC must balance these factors and find, based on the record, that a three-business-day timeframe would be more reasonable than the existing ten business days.

The Commission should retain the ten-business-day window for honoring opt-out requests that Congress prescribed.[6] CAN-SPAM's legislative history demonstrates that Congress imposed a ten-business-day timeframe because that period protected consumers while preserving some flexibility for legitimate businesses.

---

[6] In its NPRM, the FTC cites the concern of some commenters that a reduction in the timeframe for honoring opt-outs is warranted because of the possibility that a sender will, after receiving an opt-out, "mail bomb" a recipient until the ten days have elapsed. As the Commission notes, this concern is not supported by any evidence, and it is highly unlikely a business that is otherwise compliant with the Act would take advantage of the timeframe in this manner. See 70 Fed. Reg. at 25,444. Legitimate businesses would not be willing to risk the damage to their reputation that such a practice would almost certainly invite – and bad spammers do not comply with the opt-out requirements in the first place.

Describing the purpose of the Act's opt-out requirements, the Senate Report notes that "persons providing e-mail marketing services [are] responsible for making a good faith inquiry of their clients (the senders, under the definitions of this bill) to determine whether there are recipients who should not be e-mailed because they have previously requested not to receive e-mails from the sender." S. Rep. 108-102, at 18 (2003). Accordingly, the CAN-SPAM opt-out obligations were designed to require businesses to implement reasonable procedures to identify and honor the privacy preferences of consumers.

In its own CAN-SPAM rulemaking, the Federal Communications Commission set forth a 30-day window for senders to honor a new wireless domain added to the FCC's master list. See FCC Report and Order, Docket No. 04-53, at ¶ 32 (Aug. 12, 2004). In adopting this timeframe, the FCC understood that scrubbing recipient lists is a complicated and time-consuming process – essentially the same process required to honor company-specific opt-outs submitted in response to commercial e-mail messages. It is therefore not surprising that in the analogous telemarketing context, the timeframe for honoring opt-out requests is equally long – 31 days to honor new registrants on the national Do-Not-Call List, and 30 days to process company-specific do-not-call requests. See 16 C.F.R. § 310.4(b)(3)(iv); FCC Report and Order, Docket No. 03-153, at ¶ 94 (July 3, 2003).

In light of the legislative history of CAN-SPAM and analogous requirements in similar contexts, the FTC should not determine, according to the Act's requirements, that a three-business-day timeframe for honoring opt-outs is more reasonable than a ten-business-day timeframe at this point. Instead, the Commission

should retain the ten-business-day window for honoring opt-out requests that Congress prescribed. If, as technology evolves in the future, the record shows that it becomes possible to implement a shorter opt-out period without imposing a significant burden on lawful online entities, IAC would support the re-examination of this issue by the Commission.

* * *

IAC appreciates the opportunity to comment on the Commission's implementation of the CAN-SPAM Act and looks forward to continuing to work with the Commission to develop rules that best effectuate the purposes of the Act.

Respectfully submitted,

Brent Thompson
Vice President, Government Affairs
IAC/InterActiveCorp

and its Businesses

Citysearch
Classic Custom Vacations
Domania
Entertainment Publications
Evite
Expedia
Gifts.com
Home Shopping Network
Hotels.com
Hotwire.com
Interval International
LendingTree
Match.com
RealEstate.com
ReserveAmerica
Precision Response Corp.
ServiceMagic, Inc.
Ticketmaster
TripAdvisor, Inc.
udate.com
ZeroDegrees