Online Trust Alliance
an Internet Society initiative

August 29, 2017

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Ave NW
Suite CC-5610 (Annex B)
Washington, DC 20580

Filed Electronically https://ftcpublic.commentworks.com/ftc/canspamrulereview

Re: CAN-SPAM Rule, 16 CFR part 316, Project No. R711010

Dear FTC Secretary,

Thank you for providing the Online Trust Alliance (OTA), an initiative of the Internet Society, an opportunity to respond to the request for comments on the CAN-SPAM Rule. OTA's mission is to enhance online trust and user empowerment while promoting innovation and the vitality of the Internet. Its goal is to help educate businesses, policy makers and stakeholders while developing and advancing best practices and tools to enhance the protection of users' security, privacy and identity. Since its inception, OTA has been an advocate of email marketing best practices, including transparency and consumer choice and control, which are at the heart of CAN-SPAM.

This response is organized in sections that generally align with the section III, *Issues for Comment*, listed in the Request for Public Comment. Our response is informed by over a decade of working with email marketing companies, high volume senders of email, mailbox providers and consumer advocacy groups. Note that the comments reflect rough consensus from our members, while recognizing every recommendation may not be supported by every member.

Of particular interest in this response is our annual "Email Marketing Best Practices and Unsubscribe Audit."[1] This Audit, which we have conducted for the past three years, evaluates not only the compliance aspect of CAN-SPAM, but the end-to-end user experience, including the discoverability and transparency of the unsubscribe process. The Audit assesses the unsubscribe and compliance practices of the top 200 online retailers, and thus provides useful insight into the practices of top companies, though we recognize it may not be representative

[1] OTA Marketing & Unsubscribe Best Practices, https://otalliance.org/unsub

of smaller businesses. For example, in 2016, 6% of top retailers did not comply with CAN-SPAM and sent mail more than ten business days after opt-out, and 12% did not (in our judgment) provide a clear and conspicuous opt-out link.

1. Continuing Need, Benefit to Consumers

OTA believes there is a continuing need for the Rule and that it has been beneficial by setting guidelines that limit the amount of unwanted or deceptive email reaching consumers. Though the majority of spam is sent by entities who are in flagrant violation of the Rule (often from outside the U.S.), the Rule protects consumers by providing an enforcement vehicle to go after those who abuse their privilege to communicate with consumers.

It should be noted that since the inception of the Rule, the market, ecosystem and technology have evolved, changing the email landscape:

- **Receiver Sophistication.** Consumer mailbox providers (and enterprise email systems) now process and filter email based on a much more sophisticated set of algorithms, using content analysis, user spam reports, IP reputation, email authentication results and user engagement metrics (i.e., how frequently is the user opening/clicking on the email?). Getting into the inbox is not assured, and any sender must follow good practices if they want to continue to reach consumers. The result has been a decreased level of spam in the inbox.

  While we applaud the decreased amount of spam in the inbox, we do have a concern regarding the inconsistency of deliverability criteria used by mailbox providers since some are still lax in their enforcement (even when consumers tag email as spam) and others err on the "junk" side of the equation, forcing consumers to regularly scan the junk folder for messages they actually want.

- **Email Authentication.** Technologies such as Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting & Conformance (DMARC) have become widely adopted globally[2] since the inception of the Rule and are used both to verify the identity of the sender of the email and allow policy enforcement of messages that fail authentication. In fact, the FTC itself has issued a report outlining the status and best use of email authentication for businesses.[3] OTA has also tracked this adoption for over a decade, and provides annual updates as part of our Online Trust Audit.[4] For top sites, SPF and DKIM are broadly adopted, and use of DMARC

[2] Overview of Email Authentication Standards, https://otalliance.org/eauth
[3] Businesses Can Help Stop Phishing and Protect their Brands Using Email Authentication, https://www.ftc.gov/system/files/documents/reports/businesses-can-help-stop-phishing-protect-their-brands-using-email-authentication-ftc-staff/email_authentication_staff_perspective.pdf
[4] OTA Annual Online Trust Audit, https://otalliance.org/TrustAudit

is growing steadily. Though email authentication is often thought of in terms of protection from phishing, the identity element of it is useful in helping receivers build a reputation for a sender and optimize delivery decisions.

- **Sender Sophistication.** Most companies who are frequent emailers use a third-party service to send their email. These services provide a full set of database capabilities, list management, creative flexibility, preference centers/opt-downs, unsubscribe handling, analytics tracking and often deliverability services. Using these services, companies can tailor mailings to consumers' specific needs and optimize impact, deliverability and responsiveness to unsubscribe requests.
- **International Regulations.** Regulations in other countries (specifically Australia and Canada as well as the EU) have evolved. Most require an opt-in before initiating email, and are more restrictive on the unsubscribe timeframes. This is worth noting since most companies, even those based in the US, will have consumers from other jurisdictions on their mailing lists, and therefore will need to track consumers' country of residence and comply with the associated regulations. As experienced with CASL (Canada's Anti-Spam Law), senders who did not have the location of the email recipient in their files needed to get all recipients to re-opt in. A similar process may be required to become compliant with GDPR.

These market changes have forced companies to follow best practices or not make it to the inbox, which has also greatly benefited consumers. They have also allowed companies to give consumers increased choice and control and respond quickly to their feedback. In fact, the findings in our annual Unsubscribe Audit show that 94% of the top retailers honored an unsubscribe with 3 business days (85% within one business day) and nearly 60% provide a preference center or opt-down to give consumers expanded choice.[5]

2. Suggested Rule Modifications for Consumers

Though we believe the Rule in general is beneficial as is, there are a few specific areas where we believe the Rule could be enhanced to provide additional benefits to consumers without imposing extra cost on businesses.

- **Clarity on "Clear and Conspicuous."** In our Unsubscribe Audit we assess the placement, color/contrast, size and terminology used by companies to present their unsubscribe or opt-out option. Specifics vary, but in 2015 approximately 96% of top retailers had good practices in this area. Unfortunately, in 2016 this dropped to approximately 88%. The

[5] A preference center is typically a page that allows consumers to select what type(s) of email they would like to receive (e.g., topics, products, etc.) and can also include preference for frequency of email (e.g., daily, weekly, monthly). An opt-down is strictly a choice to receive email less frequently.

most noticeable drop was in the color/contrast/placement area where many opt-out links were buried in paragraphs and were hardly distinguishable from surrounding text.

Providing additional guidance or examples in this area would benefit consumers. Our criteria include placement no further than the next block of text after the content of the message, sufficient contrast to be easily seen (even on bright devices) and text no more than two points smaller than the main body text. Regarding terminology, we would suggest that "unsubscribe" or "opt-out" be recommended since many companies seem to be blurring that line with vague references.

We should also note that although "unsubscribe" is the by far the most commonly used term, in today's online environment it can create consumer confusion since it can be used to refer to a content/informational subscription of some kind as well as a promotional/newsletter subscription. We encourage organizations to clearly communicate to consumers which type of subscription they are referring to during the "unsubscribe" process.

- **Mechanism to Know Subscription Address.** Given that many consumers today use multiple email addresses which can be forwarded or delivered into a single inbox, it is important to inform them regarding which email address was used to subscribe for a given message so that they can successfully unsubscribe. In our Unsubscribe Audit, 92% of top retailers pre-populated the unsubscribe page with the associated email address – this is not only convenient and useful to avoid typo's when filling in a blank field, but also helps assure the proper email address is unsubscribed.

  Other common methods to inform the user are placing a statement in the footer of the message (e.g., "This message was sent to john.doe@email.com"), or use of the Unsubscribe header (adopted by 89% of top retailers) which in many consumer email clients presents a convenient "Unsubscribe" link in the frame of the message. Requiring some form of notification about the address to which the message was sent will reduce confusion and improve convenience.

- **Consent to Multiple Mailstreams, Provide Single Opt-Out.** We have noted several cases where sign-up to a specific company's newsletter or promotional emails generates multiple mailstreams from that sender. Examples include multiple, separate, ongoing email from different brands or lines of business of that company. In some cases, this was transparent (via a pre-checked box) and in others it was not (the consumer intent was for a specific brand/business, but the result was multiple, seemingly independent subscriptions). We believe notice and consent to multiple mailstreams is important, whether it is done through a preference center, simple checkboxes or some other form of notification.

  More importantly, on the back end, consumers should have a way to initiate an opt-out of all these mailstreams with a single opt-out request. Because consumers may have opted in to a variety of message types, we are not necessarily advocating a one-click

opt-out from all mailstreams. Rather, a best practice for this is to take the user to a page allowing them to choose which mailstreams they wish to stop. Again, in the examples we experienced, some companies allowed this (one opt-out initiating choices across brands/businesses), while others required that opt-outs be done one-by-one since they had been initiated from multiple independent entities. Ideally the mechanism used to opt-in would be synchronized with the method used to opt-out to provide a consistent user experience.

We recognize that this may not apply to cases where a consumer has opted in to "partner" offers (e.g., "if you'd like to hear from our partners, check this box") since those are initiated via a separate choice and may go to many partners. Though ideally the consumer would have a choice to opt-out of all such offers at once, realistically consumers may like some but not all of those offers, so it seems reasonable to allow them to opt-out of such offers one-by-one versus all at once.

- **Require Opt-Out Links to be Text, Not Images.** Because we have conducted the Unsubscribe Audit since 2014, we have an archive of years of consumer email messages. Looking back at them even a few months later, we can see that some of the opt-out links were presented as images which no longer render. This is confusing and inconvenient for consumers, so we recommend that opt-out links be required to be text, not a rendered image, so they have longevity.
- **Consider Extending Opt-Out Requirements to Business-to-Business Communications.** There are many examples of unsolicited business-to-business (B-to-B) communications that are framed as personal engagements (e.g., "Can I help you with your website?"), yet have no opt-out provision. Extending the Rule to cover these types of messages would significantly reduce inbox clutter. For B-to-B list mailings, the same CAN-SPAM rules could apply, with unsubscribe links required. For one-on-one B-to-B communications, individual users should be able to request to longer receive email solicitations from that solicitor. Due to its complexity, we do not recommend requiring coordination of an "opt-out" across an entire business where individuals are initiating the contact independently. The reason for this is that salespeople or others within a company may find contact information for an individual through a variety of means (e.g., public sites, LinkedIn, industry conferences, etc.) and independently contact them.
- **Clarify the Definition of "From."** The Rule currently states that the "from" line should accurately identify the sender and not be materially false or misleading. We strongly agree with this premise, but because there are many "from" addresses in an email (many are used "under the covers" in headers, email authentication, etc.) and email sent via third parties can utilize different "from" addresses for different purposes, we recommend that the definition of "From" in the Rule be specified as the "From" that is presented to the user in their email client.

3. Suggested Rule Modifications for Businesses

As described above in the discussion of current market offerings, it is not perceived that the Rule imposes undue cost or burden on businesses. Instead, market best practices are driving much of the operational realities in today's email communications. However, there are a few recommended changes to the Rule that could reduce the burden on businesses, both from a compliance overhead and a long-term liability perspective.

- **Clarification/Guidance on Types of Messages.** The Rule focuses primarily on commercial vs transactional email, and when they are combined, some guidance (and examples) on how to determine which is dominant. Since inception of the Rule, a new category of message has emerged, which could be termed "informational." This may apply to alerts about certain news items, site activity, product updates, etc. These emails should be viewed as being transactional in nature since they relate directly to the service or product that the consumer requested and clearly do not contain commercial content. However, because of the uncertainty as to whether they meet the narrow definition of transactional messages under the Rule, as a best practice many businesses provide opt-outs from these messages (to the extent they can, since some may have legal backing, such as product safety alerts). This uncertainty (and the associated costs) could be eliminated simply by expanding the definition of transactional or relationship messages to include these types of informational emails.
- **Establish a Longevity for Opt-Out Lists.** Some large emailers are concerned about the burden (liability) of carrying suppression lists in perpetuity, especially given the dynamic nature of online communications vehicles. It would seem reasonable to amend the Rule to give opt-out lists a "lifetime" (e.g., 5 years), after which the names must be purged from the system but are not subject to Rule enforcement unless the organization re-establishes a relationship with that consumer and therefore restarts the cycle. A secondary benefit is that this supports the goal of data minimization and reduces the risk of suppression lists being exposed to breaches or abuse.

4. Industry Compliance with the Rule

As mentioned in some of the recommendations above, we have conducted an Unsubscribe Audit the last three years, and therefore have a wealth of information about the practices of the top 200 online retailers. Supplementing this research is related research on native advertising and the transparency, discoverability and readability of notices.[6] Here are some highlights:

[6] OTA Native Advertising Study, https://otalliance.org/news-events/press-releases/online-trust-alliance-finds-majority-native-ads-confusing, https://otalliance.org/system/files/files/initiative/documents/2016_ota_native_report.pdf

- Compliance to opt-out has ranged from 90-98%, and was 94% in 2016. It is concerning that even 6% of top online retailers are not honoring an opt-out, since it is likely that smaller entities have even lower compliance rates.
- Nearly all retailers operate well within the ten-day Rule requirement for opt-outs. In 2016, 85% stopped sending within one business day and 94% stopped within 3 business days. The remainder did not honor the opt-out at all.
- "Clear and conspicuous" use of opt-out links was outlined in detail earlier, but it should be re-emphasized that top retailers seem to be moving in the wrong direction, so additional guidance or examples regarding the definition of clear and conspicuous would be useful.
- Unsubscribe headers are used by 89% of top retailers (growing from 76% in 2014), which translates to a visible and convenient opt-out mechanism in most consumer email clients.
- Though email authentication is not part of the Rule, it provides a foundation to allow verification of the identity of the purported sender. Approximately 95% of top retailers support both SPF and DKIM for their promotional email, and 50% have a DMARC record.

5. Reducing the Time Period for Honoring Opt-Outs

The OTA Unsubscribe Audit has validated that top retailers respond well inside the ten-day time period for opt-outs, largely due to the sophisticated systems employed to manage their email communications to consumers. It is important to note that the practices of smaller marketers have not been evaluated and they may or may not have similar compliance. Although we generally advocate for instant removal of opt-outs from mailing lists both to honor the consumer's request and to avoid the "clutter" effect on legitimate messages in the inbox that occurs when someone receives messages they've said they no longer want, based on our research, OTA currently does not recommend that this period be shortened for the following reasons:

- **Marketplace Effectiveness.** We believe that today's marketplace is effectively addressing the issue. Organizations that send email after an opt-out run the risk of being tagged as spammers by consumers, thus impacting their overall deliverability and reach. The Rule is still in place to address violators who cannot or will not comply.
- **Application to All Businesses.** While the proof points offered here point to an effective and responsive email ecosystem, there are still many organizations (primarily smaller) who handle email in a more "manual" fashion, managing it via spreadsheets or other means. Keeping the time window at ten days allows them to process opt-outs and other changes completely through their systems without incurring undue liability.
- **Unforeseen Circumstances.** Especially in the case of smaller organizations, a single system failure (or personnel absence) could dramatically impact their ability to process

opt-outs in a timely manner, so ten days gives them time to recover without increased risk of liability.

- **Additional Burden for Legitimate Marketers.** Again, though the evidence for top retailers shows strong compliance with the ten-day window, shortening this window may put an undue economic and operational burden on legitimate marketers. In today's cloud-based service environment, companies often use multiple third-party entities to conduct business, and while operation within a given cloud service may be efficient, it is often difficult to synchronize all those services quickly. Keeping the timeframe at ten days allows businesses to fully synchronize all their systems without imposing extra cost or liability exposure.

In conclusion, OTA sees great value in the CAN-SPAM Rule since it benefits consumers while promoting innovation and commerce. We recommend that it be kept in place, with the possible refinements outlined above. We also believe it is important to consider regulations in effect in other countries (e.g., Australia, Canada, EU) since any company dealing with customers in those jurisdictions will need to comply with those (generally more restrictive) regulations.

We believe industry is effectively addressing many of the day-to-day issues around email communication, and the Rule, including State rights of enforcement, is an effective deterrent to those engaging in deceptive business practices. Industry adoption of email best practices, such as those outlined in OTA's "Email Marketing Best Practices and Unsubscribe Audit," is providing consumers enhanced choice and control, setting proper expectations, increasing trust in email as an effective communication mechanism and allowing online commerce to thrive.

OTA looks forward to working with the Commission to advocate and promote these best practices.

Respectfully,

Craig Spiezle
Founder & Chairman Emeritus, Online Trust Alliance
craigs@otalliance.org
@craigspi

Jeff Wilbur
Director, OTA Initiative
Internet Society
wilbur@isoc.org