Roger Allan Ford
Associate Professor of Law

UNH School of Law
2 White Street
Concord, NH 03301

rogerford.org

Via Electric Filing

Secretary Donald S. Clark
United States Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: **CAN-SPAM Rule Review, 16 C.F.R. Part 316, Project No. R711010**

Dear Secretary Clark:

I write in response to the Commission's request for public comment on the CAN-SPAM Rule, 16 C.F.R. Part 316. I am an Associate Professor of Law at the University of New Hampshire School of Law and Faculty Fellow at the Franklin Pierce Center for Intellectual Property. I teach and write about privacy, intellectual property, internet law, and other areas at the intersection of law and technology. Among my scholarship in these areas is *Preemption of State Spam Laws by the Federal CAN-SPAM Act,* Comment, 72 U. Chi. L. Rev. 355 (2005), which was one of the first scholarly works to analyze the CAN-SPAM Act. I submit these comments in my personal capacity.

The CAN-SPAM Act set a minimum baseline for consumer protections that senders of unsolicited commercial email must respect. These protections have been largely effective at giving consumers the ability to manage how a large group of companies uses their email addresses for marketing. At the same time, the Act has had little effect on the volume of unsolicited commercial email or on the amount of email sent by scammers and fraudsters. The Act and its implementing Rule, then, have been neither the success they should be nor the failure that critics describe.

The Commission should adjust the Rule to maintain its substantial consumer benefits while addressing its shortcomings. By leaving in place the significant consumer protections the Rule provides while updating and tweaking their substance to provide additional protections and account for technological change since the Rule was promulgated, the Commission would best implement the goals and structure of

the Act. Moreover, the Commission should look for additional ways, within its authority under the Act and other statutes, to address the problem of scam emails.

The Can-Spam Act is neither the success it should be nor the failure its critics describe.

Congress enacted the CAN-SPAM Act in 2003 to address two problems. As the Internet grew into a part of everyday life, unsolicited commercial email, or spam, made up an increasing share of email traffic, amounting to more than half of all emails sent and clogging inboxes around the world. At the same time, growing state efforts to address the problem threatened to hinder email's usefulness as a tool of commerce by making it difficult and expensive to comply with fifty different state laws. By setting a uniform baseline level of consumer protections with which companies sending commercial email must comply, the Act aimed to reduce the volume of spam and give consumers tools to control the amount of spam they receive.

It did not work out as Congress intended. The CAN-SPAM Act did not eliminate or even significantly reduce spam, which still accounts for more than half of email traffic. And though the Act did create a uniform baseline level of consumer protections, many senders ignore those protections. Even when companies do obey the Act, its rules have proven insufficient to reduce the costs that spam imposes on recipients. The Act, then, has not been the success it should be.

At the same time, the Act has successfully defined the rules of the road for legitimate senders of commercial email—a role that should not be ignored. Before the Act, email users had no legal right to control their own email inboxes; a company could send unlimited commercial email, without consent, and face no legal consequences or constraints. It could purchase or build a list of addresses, send them as many emails as it felt like, decline to offer any option to opt in or out of receiving emails, and refuse to provide any way to get in touch with the sender, all without any accountability for its choices. After the Act, senders must disclose their name and address, offer a way to opt out of receiving further messages, and label messages containing adult content. These are valuable consumer protections.

There are two kinds of spammers: Legitimate companies that generally comply with the law and illegitimate scammers that are unlikely to comply no matter the Rule's content.

The key to understanding the Act's mixed effects, and building on its successes while addressing its shortcomings, is to understand that not all unsolicited commercial email is the same. Instead of one unified market of spammers, there are different kinds of companies sending different kinds of unsolicited commercial email. Some of these companies are legitimate businesses that generally comply with the law; with these companies, adjustments to the Rule are likely to affect consumers, for good or ill. Other companies that send commercial email are illegitimate scammers that are unlikely to comply with the Act no matter what it says; with these companies, other approaches are needed.

The first category, legitimate companies that generally comply with the law, includes many companies and groups using email as part of their marketing strategies. Most of these companies use email for marketing in ways that would not be recognized as classic spamming. Few legitimate companies send email indiscriminately to every email address they can get their hands on, since doing so might offend customers and would quickly get them blacklisted by email services. Rather than using email marketing to develop new customers and leads, where the costs usually outweigh the benefits, they use email to market to those who are already thought to be interested in the company's products—existing customers, people who sign up for their mailing lists, customers of related businesses, and, most controversially, people whose browsing behavior or demographic profile indicates that they are likely to be receptive to the sender's message. Someone who has bought items in the past from an online store, or booked hotel rooms with a chain, might get emails touting promotions, or other products the recipient might be interested in, or destinations she might enjoy. Someone who has bought items from one store might also get emails from that store's corporate siblings. And someone who has given money to one organization or political campaign might get emails from other groups or campaigns that are ideologically or politically aligned.[1]

---

1. This category consists of legitimate companies that send unsolicited commercial email, but many companies that send *solicited* commercial email—for instance, newsletter providers or companies that send periodic results in response to saved searches—also comply with the Act out of an abundance of

Congress's decision to allow email marketing, while requiring senders to adhere to specific consumer protections, reflected a balance between two competing concerns: its desire that users have control over their email inboxes and its judgment that email could nevertheless be a legitimate part of a company's marketing strategy. The latter concern required a federal law, since some states at the time were moving toward banning spam entirely. The Act preempted almost all state anti-spam laws, giving companies a uniform set of rules for email marketing—rules with which legitimate companies generally comply.

The second group sending commercial emails consists of scammers who are unlikely to comply with the Act and the Rule regardless of their contents. This group likely sends the bulk of unsolicited commercial email. Some of these scammers are companies while others are individuals and loose groups of conspirators. These scammers hawk prescription drugs from online pharmacies, counterfeit watches, adult services, and all manner of scammy products and services. And unlike legitimate companies targeting existing customers and others likely to be interested in a company's services, these scammers send as many emails as they can, switching servers and playing cat-and-mouse games with spam-blocking services to get their messages in front of users.

Unlike with legitimate companies using email as part of their marketing strategies, there is no reason to think Congress intended these scammers to be able to operate legally, and for the most part they make no effort to do so. Besides simply selling products that can be illegal (like illegal drugs, legal prescription drugs without a prescription, and all sorts of counterfeit goods), these emails often fail to include information required by the Act (like the name and mailing address of the sender), use false sender and header information to disguise their origins, and include false and deceptive content (often hidden when the email is seen by a user) to fool spam-filtering software. These actions are both prohibited by the Act and by state laws that are carved out of the Act's preemption clause; they also likely violate other laws, like various consumer-protection laws and the prohibition on wire fraud.

---

caution. These companies can be especially hard hit when companies violate the Act with impunity, since the result is more email users relying on technological filtering, and it can be difficult for spam-filtering algorithms to differentiate between solicited and unsolicited email.

This two-part nature of the email ecosystem stems from the basic structure of the technologies upon which email is built, which require no authentication of senders and give users little ability to decide who can email them.[2] This structure has its origins in design decisions made decades ago in contexts that were strikingly different from those in which email is used today. Email is not a symmetric, negotiated transaction, where a sender and a recipient must come to an agreement before a message can be transmitted. Instead, under the commonly used SMTP, POP, and IMAP protocols, a sender can unilaterally send an email, which a recipient's mail server will receive and, usually, place in the recipient's inbox. Developers have created various authentication and filtering technologies, grafted on top of these protocols, but these tools are not universally adopted and they work imperfectly at best. This has two important consequences: it means that there is no technical impediment to sending spam, and it makes it difficult or impossible to track down senders of spam messages.

Since these two kinds of unsolicited commercial email, and their senders, are so different, they require different legal responses, as discussed below.

With respect to email from legitimate companies, the Act has provided substantial consumer benefits, though updates are needed.

In reviewing the CAN-SPAM Rule, the Commission should recognize that when it comes to email from legitimate companies, the Act and its implementing Rule have provided substantial consumer benefits that should be maintained. At the same time, updates are needed to strengthen those benefits and respond to changes in the market for email marketing and in online technologies.

---

2. The Commission recognized this problem in its June 2004 report to Congress on a national "do-not-email" registry, which recommended against implementing such a system. *See infra* page 9. The Commission expressed concern that without server-level authentication of email senders, such a registry could be used by spammers to verify email addresses for targeting, and suggested creating a registry only after the market moved to an authentication-based email system. FTC, *National Do Not Email Registry: A Report To Congress* (June 2004), *available at* https://www.ftc.gov/sites/default/files/documents/reports/can-spam-act-2003-national-do-not-email-registy-federal-trade-commission-report-congress/report.pdf.

The principal consumer benefit of the Act and Rule has been to give email users a degree of legal control over their inboxes, which is critical because they have no similar technological control. These legal controls have been the major tool allowing people to control how companies can use their inboxes for marketing. Without those controls, companies can send marketing emails, clogging up recipients' inboxes and using their resources—in time, network traffic, data storage, and so forth—without permission and without any obligation to stop, ever. Email before the Act was not an opt-in or an opt-out system; it was a no-choices-at-all system, unless an email sender chose for its own business reasons to offer users the ability to remove themselves from the sender's list. Under the Act, in contrast, senders must offer recipients the ability to opt out of receiving emails; must disclose their names and addresses; and must label emails containing adult content. The Act also prohibits various methods used by spammers to build email lists and evade detection, though few legitimate companies would be likely to use such methods even if they were legal.

The Commission should build on these protections so that the benefits they have provided consumers remain strong. Specifically, the Commission should take three actions, consistent with the Act, to protect consumer choice and further Congress's goals in enacting the Act.

Clarify the opt-out requirement. First, the Commission should use its rulemaking authority under section 13 of the Act to clarify the Act's requirement that email senders provide a "clearly and conspicuously displayed" mechanism to opt out of future messages.[3] This requirement should be updated in two ways: by imposing type-size and visibility requirements for unsubscribe links and by mandating a standardized opt-out mechanism that can be invoked by a user's email client software. Type-size and visibility requirements are necessary because although legitimate senders have largely honored the Act's requirement that they provide opt-out mechanisms, many have honored in the breach the requirement that those mechanisms be "clearly and conspicuously displayed." Instead, senders routinely bury unsubscribe links in lengthy fine print at the bottom of an email, in grey type on slightly lighter grey backgrounds. For example, these screen shots show how senders typically bury opt-out instructions:

3. 15 U.S.C. § 7704(a)(3)(A).

Email Management Area

Please do not reply to the address you received this email from. Manage your email communications below.

Why you received this email message:

You are subscribed to the NLJ Legal Times Afternoon Update as [redacted]. You may be subscribed to multiple publications as part of your relationship with us.

To stop receiving the NLJ Legal Times Afternoon Update (unsubscribe) or to update your email marketing preferences, please click here. On this page, please update your subscription choices to this publication, and any others you may receive. You may also change your opt-in of email marketing promotions from ALM. It may take up to 10 days for your changes to take effect.

How to contact us should you have questions:

The National Law Journal®
120 Broadway, 5th Floor,
New York, NY 10271-1101
Customer Service Phone: 1-877-256-2472

About ALM | Customer Support | Privacy Policy | Terms & Conditions

Agora Financial

If you believe you have received this email in error or no longer wish to receive this type of e-mail, you can unsubscribe by clicking here Nothing in this e-mail should be considered personalized investment advice. Although our employees may answer your general customer service questions, they are not licensed under securities laws to address your particular investment situation. No communication by our employees to you should be deemed as personalized investment advice. We expressly forbid our writers from having a financial interest in any security recommended to our readers. All of our employees and agents must wait 24 hours after on-line publication or 72 hours after the mailing of printed-only publication prior to following an initial recommendation. Any investments recommended in this letter should be made only after consulting with your investment advisor and only after reviewing the prospectus or financial statements of the company.

*Limited quantities available while supplies last. Cannot be combined with any other offers or promotions, except free shipping (where applicable).

**Excludes dining seating, beds, benches, office chairs, outdoor furniture and clearance items. Cannot be combined with any other offers or promotions.

To make sure our email updates are delivered to your inbox, please add crateandbarrel@mail.crateandbarrel.com to your email Address Book.

Unsubscribe
To unsubscribe from our email list, just click here.

Privacy policy
Click to view our privacy policy.

This email may be considered an advertising or promotional message.

Crate and Barrel, 1250 Techny Rd, Northbrook, IL 60062

In none of these emails is the mechanism to opt out of future emails "clearly and conspicuously displayed."

To remedy this problem, the Commission should require senders to include a standardized box containing information on how to unsubscribe, at the bottom of each email, akin to other standardized labels for food, drugs, and cigarettes. For instance, such a box could look like this:

CAN-SPAM Information

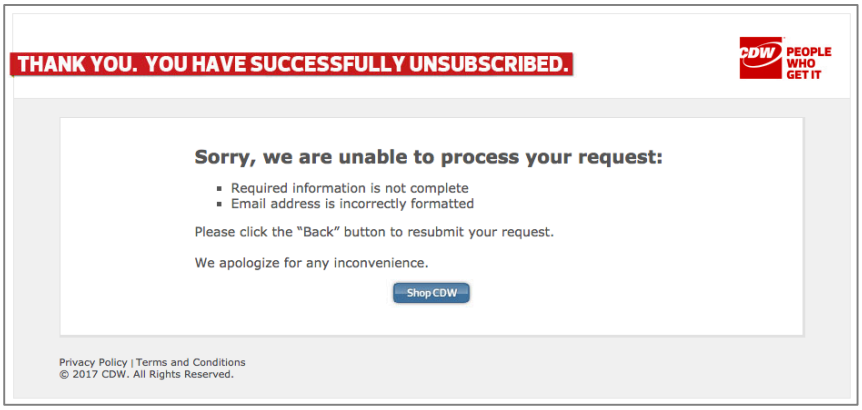
This email was sent to bill.smith@email.com by XYZ Inc., 123 Main St., Chicago IL 60601.

To unsubscribe from this mailing list, click here.

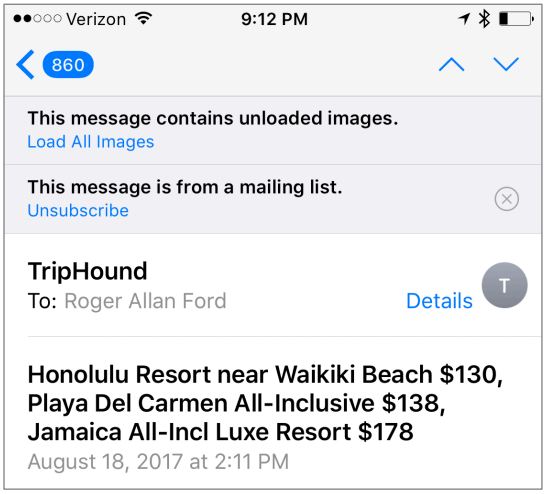
To stop all emails from this sender, click here.

Besides being clearer and more conspicuous than the current plethora of hidden unsubscribe links, a standardized box would save time and help email users better express their preferences, since users would come to recognize and know how to use the standard box instead of having to search for each email's distinct unsubscribe instructions.

Besides simplifying the opt-out process for users, a standardized opt-out mechanism would also be more likely to work reliably, which would help solve the all-too-common situation in which an email's opt-out mechanism fails to work, thanks to server-side errors or other (intentional or unintentional) bugs. For instance, I recently received this internally contradictory message when opting out of email from a sender that started sending me email without any existing commercial relationship:



Moreover, mandating a standardized opt-out mechanism that can be invoked by software would allow consumers to use third-party tools to manage their email accounts in one place, rather than going message by message to opt out. There is a clear market demand for such tools. For instance, email clients from companies like Apple and Google have started offering users the ability to unsubscribe from a mailing list with one click, as shown below:



But this functionality depends on companies figuring out how to parse, and invoke, different email senders' different unsubscribe options. If one sender's option sends users to a webpage to unsubscribe, and requires them to check a box or hit a specific button to do so, the program must figure that out; if another requires typing in one's email address, it must do that instead. And because these opt-out mechanisms are not standardized, programmatic options are inherently unreliable and likely to be implemented only by a few companies. A standard opt-out mechanism that could be invoked without error or uncertainty, in contrast, would lead to a more competitive market for email software, giving customers better choices about how to manage their inboxes.

Reconsider creating a "do-not-email" registry. Second, the Commission should reconsider its previous decision declining to create a "do-not-email" registry pursuant to Section 9 of the Act, 15 U.S.C. § 7708.

The Commission elected not to create such a registry in 2004, reasoning that email's lack of any server-level authentication meant that a registry could be

counterproductive because "spammers would most likely use a Registry as a mechanism for verifying the validity of email addresses and, without authentication, the Commission would be largely powerless to identify those responsible for misusing the Registry."[4] The Commission instead decided to encourage and wait for the widespread adoption of email systems with built-in authentication.[5] Since that time, progress has been made on server-level authentication through tools like DKIM and SPF authentication, which are used by large email providers to verify sender domains. Although those tools have not yet been widely enough adopted to end the need to accept unauthenticated email, they are used by providers like Google, Yahoo, and Microsoft that provide email service to millions of users. The adoption of such tools would help resolve the issues that led the Commission to decline to create a "do-not-email" registry in 2004. Given this change in technology, then, the Commission should reexamine its decision not to create a registry, since doing so would provide substantial value and since the downsides emphasized by the Commission are likely to decline or to be overstated.

A "do-not-email" registry would enhance consumer welfare by making it easier for email users to give effect to their email preferences. The Act gives users the ability to choose whether to receive email from a commercial sender, but making that choice requires an individual sequence of steps for each sender—steps that are often specific to each sender. An email user who wants to receive as little email as possible, then, has to unsubscribe to email from each individual sender, which can take a substantial amount of time and effort. A registry, in contrast, would let a user indicate this preference once, not over and over. This time savings is exactly why Congress directed the Commission to create a National Do Not Call Registry, and it is equally applicable to email.

The Commission concluded that the benefits of a registry were outweighed by the risk that spammers would use it to verify email addresses and target them for more email. In addition to the growth of authentication systems, though, other modern technical tools mean that that risk is avoidable. Rather than hand over the contents of a registry, the Commission could require companies to submit email addresses that have been processed by a cryptographic hash function like the MD5 or SHA-2

---

4. FTC, *National Do Not Email Registry: A Report To Congress, supra,* at i.
5. *Id.* at ii.

algorithm. A cryptographic hash function takes an input, like an email address, and generates a fixed-length value that cannot feasibly be converted back into the input; tech companies routinely use such hashes in applications like verifying user passwords. My email address, roger.ford@law.unh.edu, for example, generates the MD5 hash value 76905da1ac54406ddbf38acf85eadbf3. A company that wanted to a "do-not-email" registry could hash each email address on its mailing list, compare them to the hashes provided by the registry, and remove any matches from its mailing list. And the nature of the algorithm means that a spammer could not go the other way: given a hash value, one cannot feasibly obtain email addresses to spam. If a spammer generated a list of possible email addresses, it would be possible to verify which of those addresses were on the list, but doing so wouldn't be any more useful than just emailing every possible address in the first place.

Cryptographic hashes are just an example; the point is that there are technical solutions to the problems the Commission identified in 2004. The Commission should consider, then, ways to provide the value of a "do-not-email" registry while overcoming the problems that stopped it more than a decade ago.

Provide preemption guidance. Third, the Commission should provide guidance to states and others on the scope of the Act's preemption provision. The Act preempts most, but not all, state spam laws: it supersedes any state or local law that "expressly regulates the use of electronic mail to send commercial messages, except to the extent that [the state or local law] prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto."[6] This provision preempts, then, state laws that would prohibit all unsolicited commercial email. It nevertheless leaves important openings for states to have a role combatting the spam problem—openings that have been underappreciated.

There are two key roles states could play that would rely on the preemption clause's exceptions. First, states could enact laws prohibiting falsity or deception in commercial emails: in the subject line or contents of the message, or in its routing information and from address. Many such emails will already violate the Act, but not all will do so, since the Act prohibits forged headers and deceptive subject lines but

6. 15 U.S.C. § 7707(b)(1).

not other forms of deception.[7] States, then, could play a useful gap-filling role in prohibiting other kinds of falsity or deception, like in the contents of commercial emails. And second, states could provide for penalties and enforcement mechanisms that go beyond those in the Act. The Act's enforcement provisions are limited: the Commission, state agencies and attorneys general, and ISPs can bring civil actions;[8] there is also a narrow criminal provision.[9] Most violations of the Act, though, are not crimes, and recipients of emails that violate the Act have no recourse. States could overcome these limitations by providing for criminal penalties and private rights of action for email recipients. Without assurance from the Commission that states have that authority, though, they are less likely to become involved in an area where the federal government appears to have occupied the waterfront.

With respect to email from scammers, the Commission should do more.

When it comes to the second category of spam email—that from scammers who are unlikely to comply with the Act and the Rule in any circumstance—the Commission should recognize that the Act is unlikely to have a significant effect, and so look for other ways to exercise its authority to help reduce the spam problem.

The most significant thing the Commission could do to combat spam might be to facilitate the widespread adoption of authenticated email standards. This is an option the Commission contemplated in its 2004 report, but has not undertaken. In that report, the Commission contemplated such a standard as facilitating the creation of a "do-not-email" registry, but it would also directly reduce spam, since it would both facilitate technological solutions like filtering and facilitate enforcement actions under existing law like the Act.

In its 2004 report, the Commission observed that "[t]he private market is already moving toward creating systems for authenticating that an email message actually comes from a mail server operated by the second-level domain appearing in the

7. 15 U.S.C. §§ 7704(a)(1)–(2), 7705.

8. 15 U.S.C. § 7706.

9. 15 U.S.C. § 7704(d).

message."[10] Though the Commission was right that authentication would become more common, in the 13 years since, the market has not embraced mandatory authentication, and it is time for the Commission to consider how its "support may help accelerate the pace" of adoption.[11] Although mandating adoption of specific technical protocols is not likely to be the best approach, the Commission has other tools in its toolkit, including standards certification, encouragement of large ISPs through tools like industry summits, and its unfair-trade-practice authority under the FTC Act. Indeed, the Commission has made laudable use of that authority to encourage adoption of industry-standard security measures; insecure email is one of the largest security risks today for most computer users.

The Commission could also take meaningful action against scam emails by sponsoring a Spam Challenge along the lines of its successful Robocall Challenge and subsequent challenges, which developed new technical tools to fight robocalls. The market has developed robust anti-spam tools like filtering, but those tools suffer from inherent limitations due to the decentralized nature of email services, HTML and JavaScript obfuscation, and other limitations that make it hard to reliably sort spam and non-spam emails. The Commission is well positioned to bring stakeholders and technologists together to find and develop new techniques and tools both for filtering messages that violate the Act and for preventing such emails from being sent in the first place.

Finally, the Commission could look for ways to use payment processors and other critical intermediaries to reduce the amount of illegal spam sent. This could take several forms. The Commission could work with intermediaries to discover and shut down accounts belonging to spammers; or, if intermediaries are not cooperative, it could prioritize enforcement actions against those parties. These steps could prove effective because illegal spam is a commercial enterprise just like legal spam: it doesn't work if there isn't some way to make money from the effort. So payment processors and other intermediaries provide crucial links between senders, who seek to sell goods and services, and recipients, who seek to pay for those goods and services.

---

10. FTC, *National Do Not Email Registry: A Report To Congress, supra,* at 35.
11. *Id.*

* * * * *

Thank you for the opportunity to comment on the Commission's review of the CAN-SPAM Rule. This review is an important opportunity to build on the substantial consumer benefits the Act and Rule have provided while adjusting them to take account of the effects of a decade and a half of evolving technology. By building on what has worked and trying something new where the Act and Rule have not worked, the Commission can continue to fight illegal spam while giving consumers tools to protect their own privacy and control of their email inboxes.

Sincerely yours,

/s/
Roger Allan Ford
Associate Professor of Law
University of New Hampshire