

August 31, 2017

Federal Trade Commission

Title: Rule Review; Request for public comments.

Subject Category: 16 CFR Part 316; CAN-SPAM Rule: Rule Review; Request for Public Comments; Project No. R711010

**VIA ONLINE SUBMISSION:** <https://ftcpublic.commentworks.com/ftc/canspamrulereview/>

For itself and on behalf of similarly situated, small to mid-sized Internet service providers, XMission, L.C., proposes the following modification to the CAN-SPAM Act for the interest in efficiency and benefit of the Act to consumers and small business, as well as for the purpose of creating a more compliant commercial email marketing industry.

**Current Definition of “Procure” affecting private party actions:**

Action by Internet access service

“(2)SPECIAL DEFINITION OF “PROCURE” In any action brought under paragraph (1), this chapter shall be applied as if the definition of the term ‘procure’ in section 7702(12) of this title contained, after ‘behalf’ the words ‘with actual knowledge, or by consciously avoiding knowing, whether such person is engaging, or will engage, in a pattern or practice that violates this chapter’”

15 U.S.C. §7706(g)(2).

The complete definition is as follows:

Action by Internet access service

“The term ‘procure’, when used with respect to the initiation of a commercial electronic mail message, means intentionally to pay or provide other consideration to, or induce, another person to initiate such a message on one’s behalf ‘with actual knowledge, or by consciously avoiding knowing, whether such person is engaging, or will engage, in a pattern or practice that violates this chapter.’” 15 U.S.C. § 7702(12), § 7706(g)(2).

**Proposed Modification:**

The elimination of the 7706(g)(2) language from the definition of “Procure” where the plaintiff is a private *bona fide* Internet service provider. Plaintiff Internet service providers should be held to the same standard as FTC or government plaintiffs.

**Proposed 16 CFR 316.7 Procurement for Private Actions by Internet Service Provider.**

The extended definition of “Procure” found in 15 U.S.C. § 7706(g)(2) does not apply to private party actions where the plaintiff is a *bona fide* Internet service provider. In such cases, the definition of “Procure” shall be that found in 15 U.S.C. § 7702(12) without modification. The extended definition of “Procure” remains in effect for all other private party actions.

I. XMISSION'S HISTORY AND EVIDENCE OF NEGATIVE IMPACT OF SPAM.

**Brief History of XMission**

1. XMission was founded in 1993 as Utah's first Internet service provider ("ISP").
2. From its early days as a private, Utah ISP to its current role as a global business Internet provider, XMission has expanded its technical offerings to include sophisticated cloud hosting, web hosting, email service and hosting, collaboration tools, business VoIP phone service, and high speed internet connectivity solutions including optical Ethernet, copper and fiber.
3. Throughout its history, XMission has also worked with hundreds of Utah's nonprofit organizations by providing free services, and by sponsoring a variety of community-based events and facilities.
4. XMission is a widely known and well-recognized ISP in Utah.
5. In cooperation with Salt Lake City government, XMission provides free WiFi to the downtown Salt Lake City metropolitan area.
6. XMission currently has 37 employees.
7. XMission owns all the servers, routers, and switches on its network through which it hosts and provides its Internet access services for its customers.
8. XMission has an expansive network and infrastructure, which it has had to consistently update, upgrade and augment in order to combat ongoing spam problems.
9. XMission is the sole owner of all its hardware, and has complete and uninhibited access to, and sole physical control over, the hardware.
10. XMission provides Internet access services to both commercial and residential customers.
11. The email accounts hosted and served by XMission include email accounts owned by third-party customers of XMission, email accounts owned by employees and/or customers of XMission's third-party customers, email accounts owned by employees of XMission, and also email accounts owned by XMission itself.
12. On average, XMission's network consists of approximately 50,000 main accounts with 13,300 billable entities.

**Harmful Effects of Spam**

13. Throughout its business history, XMission has expended well in excess of \$3,000,000 in hardware acquisition, maintenance and related expenses to increase capacity to deal with increased SPAM and related harm, SPAM filtering expenses, and employee time in dealing with problems caused by its receipt of SPAM generally.

14. XMission expends, on average, over \$285,000 per year in dealing with SPAM related issues and associated employee time, exclusive of attorney fees. This is a significant burden on a mid-sized ISP like XMission.

15. XMission has two full-time employees whose primary responsibilities are to deal with SPAM related issues, including, adjust filtering, responding to customer complaints, addressing blacklist issues, and acting as first responders to data security breaches, and hardware issues caused by SPAM.

16. XMission also employs 12 other technicians and one supervisor who dedicate at least part of their time to dealing with the aforementioned SPAM issues.

17. XMission currently has 13 servers dedicated specifically to process SPAM. Those servers could be dedicated to providing XMission's Internet access services if it were not for the SPAM. XMission has had more total spam-mitigation servers over its history.

18. Receiving an e-mail is a simple transaction. If it's wanted e-mail, it just gets copied off of the Internet and put into a file. If it's spam, XMission have to go through and analyze it against databases, against word counts, and against filtering rules. For every email, it's more intensive to identify spam than it is to identify wanted e-mail. Half of XMission's servers would not be required if there was not unwanted e-mail. In such a scenario, XMission can confidently say that it would need 20% of the resources it currently uses in handling e-mail.

19. Approximately 13% of all general technical support staff time and 39% of mail administrative time is necessarily dedicated to dealing with SPAM related issues.

20. Daily, between 40% and 85% of the email messages that XMission receives on its system are SPAM emails. Historically, XMission estimates an average spam level of 60% of all email hitting XMission systems.

21. The percentage of SPAM emails would be significantly higher if not for all the precautions that XMission has taken, including subscribing to leading anti-spam services, including blacklists such as URIBL and Spamhaus, in addition to creating customized and proprietary filtering rules and email server configurations utilizing tools such as SpamAssassin, which all come with significant expense.

22. The harm XMission suffered, and continues to suffer, as result of the ongoing SPAM problem, is manifested in financial expense and burden significant to XMission; lost employee time; lost profitability; the necessity to purchase and dedicate equipment specifically to process SPAM that could otherwise be dedicated providing internet access services; harm to reputation; harm to XMission's goodwill; and customer and e-mail recipient complaints.

#### **XMission's Spam Litigation Efforts**

23. XMission became aware of the CAM-SPAM Act in or around 2013.

24. Between 2013 and 2017, XMission has initiated 10 lawsuits against parties who, in some way, were responsible for sending spam emails in violation of the CAN-SPAM Act.

25. In every lawsuit where an Answer or responsive pleading was filed, the Defendant relied heavily on the definition of "Procure" set forth in 7706(g)(2) in order to pass responsibility to other, unidentified email affiliates. Essentially, the argument was that the Defendant who was either the party whose product, service or website was being advertised, or the party who controlled the advertisement network responsible for facilitating the email advertising, was not liable because they passed the responsibility for actually clicking send to other parties.

26. XMission's anti-spam efforts have come at great expense. To date, XMission has expended in excess of \$1,000,000 on attorney's fees in an effort to mitigate the harmful effects of spam on its business.

27. In analyzing its spam volume generally pre and post-litigation, it appears that XMission's public litigation efforts have only resulted in a very modest effect on spam generally. However, the dip in spam is not statistically significant enough to determine if such is the result of a normal lull or as the result of XMission's visibility through litigation and corresponding fear by wrongdoers.

28. Despite XMission's public efforts, there does not appear to be any significant effect industry wide as the types of can-spam violations (specifically relating to false or inaccurate header and registration information) in email received today are the same as those received prior to XMission's litigation efforts.

29. In fact, during its history, XMission has had occasion to deal with the various companies on more than one occasion for the same types of CAN-SPAM violations despite having reached out of court compromises with them in prior years. In other words, the risk of harm from litigation to those violating the law appears to be outweighed by the financial benefit derived from email marketing campaigns that violate the law.

## II. EFFICIENCY AND BENEFIT OF ACT AS CURRENTLY STATED AND BASIS FOR MODIFICATION

The Request for Comment Project No. R711010, seeks comments on the following questions:

"3. What modifications, if any, should be made to the Rule to increase its benefits to consumers?"

"8. What modifications, if any, should be made to the Rule to increase its benefits to businesses, including small businesses?"

"10. What modifications, if any, should be made to the Rule to reduce the costs imposed on businesses, including small businesses?"

### **Proposed Modification**

As set forth above, XMission proposes a modification regarding 7706(g)(2). Specifically, that the extended definition of “Procure” found in 15 U.S.C. § 7706(g)(2) does not apply to private party actions where the plaintiff is a *bona fide* Internet service provider. In such cases, the definition of “Procure” shall be that found in 15 U.S.C. § 7702(12) without modification. The extended definition of “Procure” remains in effect for all other private party actions.

### **Consumer and Small Business Benefit**

Currently, under the CAN-SPAM Act and governing case law (i.e., *Gordon v. Virtumundo*, 575 F.3d 1040 (9th Cir. 2009)), an individual consumer does not have a private right of action. See 15 U.S.C. § 7706. The only parties with rights of action are certain Federal Agencies (15 U.S.C. § 7706(b)), the FTC (15 U.S.C. § 7706(d)), States (15 U.S.C. § 7706(f) and Internet access services (15 U.S.C. § 7706(g)). Internet access services can include anyone who provides access to information or content online, such as websites, social networks, email service providers and, prototypically, ISPs.

Government and FTC are not actively pursuing CAN-SPAM claims and are therefore, not bringing any significant benefit to consumers or small businesses.

In the 14 years of the CAN-SPAM’s existence, there appear to have been only 26 CAN-SPAM actions filed by various branches of the government. The vast majority of those actions were filed within the first few years of the CAN-SPAM Act’s existence. The actions appear to have been based on the types of products advertised and not necessarily related to the types of email practices employed. As an example, of the 26 cases, essentially three product categories were represented: pornography, debt relief, and dietary supplements.

XMission, a *bona fide* ISP, receives hundreds of thousands of spam emails per month. The emails span nearly every industry. Litigation based on product category does not address the actual core problem, which is email marketing practices that are designed to bypass spam filters, invade email inboxes and entice consumers to open email messages. These practices are industry wide and pervasive across all product categories and not limited to those found offensive (or worthy of prosecution) by the FTC or States.

The ISP stands at the threshold of all email communication. All emails are processed directly on their servers and they are in the best position to seek enforcement of the law for violations regardless of industry type and location. In the case of direct consumer protection and benefit, only the ISP has the ability to assert claims against violators of the law. The ISP provides the direct access to the Internet, and it is the ISP who carries the burden and expense of the spam across its network (also including for other possible Internet access services who reside on ISP networks, such as social networks, website and email service providers). Ultimately it is the customer’s relationship with the ISP that will be strained and damaged as the result of spam.

Among all parties vested with a right of action, the ISPs are the best situated to protect consumers and ensure consumer benefit of the CAN-SPAM Act. There is no reason why a violator of the law should have an additional layer of defense (i.e. special definition of “Procure”) when an action is brought by a *bona fide* ISP, as such ultimately places a harder burden on the ISP than that imposed on government or States.

**Statements from a Large Industry Player in Public Proceedings Reflects the Industry's Attitude Toward CAN-SPAM Compliance in Private Party Actions.**

“Adknowledge is a large company. It is fourth in the world behind three other ad networks, Google, Yahoo, Microsoft, and then comes Adknowledge. Adknowledge connects advertisers with publishers. Publishers are not limited to e-mail marketers. They might be mobile games that you play on your phone. They might be a video channel on YouTube. It might be a blog. It might be a Web site. Adknowledge has these relationships, lots of relationships. So Google, for example, has the eyes of ten billion consumers, or the like. Adknowledge has the eyes of two billion consumers. . . . One type of marketing that it does and it's very good at is connecting advertisers with e-mail publishers. The reason it's so good at that is Adknowledge has robust terms and conditions, practices and policies, and agreements. It requires every publisher to agree to certain things.”

*Transcript of Hearing on Motion for Injunction, U.S. District Court for the District of Utah, Case No. 2:15-cv-277, 54:14-25 – 55:1-7.*

14. In online advertising, a “publisher” is the owner of some distribution mechanism with direct relationships with its users. Examples of publishers include online merchants, personal websites, social network websites, app/game developers, list owners—basically anyone with an on-line avenue for reaching the attention of people. Publishers earn money from their content by delivering ads to users and get paid by advertising networks.

15. For purposes of online advertising, an “advertiser” is the party seeking to advertise its services or products. Although some publishers may also be advertisers (an online store selling products is often both), this is not always the case. Advertisers rely on relationships with marketing networks to funnel ads through publishers to users.

16. Adknowledge is functionally a “marketing network” and maintains relationships with innumerable advertisers and publishers. Adknowledge uses the vast data and complex analytics it has developed to efficiently connect the right advertisers to the right publishers, so ads can be directed to the most suitable customers. Advertisers pay Adknowledge for access to its data and publisher network.

17. Adknowledge’s email business pays publishers a commission when the publishers’ users click on Adknowledge ‘redirect links’ resulting in clicks, page views, or purchases for advertisers, for which Adknowledge itself is paid. . . .

19. For Adknowledge’s publishers, Adknowledge is not the legislative sender, thus Adknowledge has no knowledge, rights, or control over to whom or even if publishers send email. Just to be clear, because Adknowledge’s network requires encrypted IDs representing email addresses, Adknowledge has no specific knowledge of where and to whom its publishers deliver email. Like other large online advertising companies—including Google and Yahoo—Adknowledge has no direct relationship with its publishers’ users, relying instead on publishers to curate their own relationships with their own users and customers.

20. All Adknowledge publishers are required to represent and warrant to Adknowledge that their activities comply with all applicable federal and state laws and regulations, including specifically the CAN-SPAM act.

26. Adknowledge is not the sender of commercial email and cannot directly control where its publishers direct email.”

*Declaration of Matt Hoggatt, General Manager of Adknowledge’s email business, Case 2:15-cv-00277 (ECF 15) (emphasis added).*

Adknowledge, one of the largest players in the email-marketing industry, understands very well the nuances of the special definition of “Procure.” Even though it admittedly controls the commercial emailing to billions of people, in private party CAN-SPAM litigation, it passes the buck for compliance to its unnamed affiliates. *See* cited paragraphs 19-20, 26 above. The special definition of Procure allows this to occur when a private ISP like XMission brings an action. However, if the action were brought by FTC or government, no special definition would apply. Such results in inconsistent standard for compliance and creates a much more difficult task of enforcement by the party who is in the best position to enforce the law, the ISP.

### III. CONCLUSION

XMission is the quintessential small-business ISP. Its burden as the result of its receipt of spam email is significant as set forth in Facts section above, resulting in millions of dollars spent combating unlawful spam against violators of the law who simply attempt to pass responsibility to their hired affiliates. As the result of the special definition of “Procure,” litigation against the biggest industry players--those who actually control the spam market--has little effect on actual compliance at the control level. As long as the special definition of “Procure” exists for private ISP actions, and as long as FTC and government are inactive in their prosecutorial efforts, the industry leaders will continue to shirk responsibility for non-compliance and simply pass all responsibility to the fungible, dime-a-dozen email publishers, resulting in millions of dollars of expenses associated with spam processed by ISPs.

The proposed modification would hold private ISPs, such as XMission, who bear the burden of spam and also who stand in the strongest position to protect the consumer experience, and who are essentially acting as private attorneys general, to the same enforcement standard as FTC or state prosecutors.

Importantly, the modification would not result in any increased cost to the email marketing industry because the compliance requirements would not change, they would simply have to be followed. The modification would create a smoother path to enforcement of the existing law for ISPs, and a more compliant commercial email industry generally.

Respectfully Submitted,

Peter Ashdown  
President XMission, L.C.