ESPC
Email Sender & Provider Coalition

May 26, 2016

Via Electronic Submission to http://apps.fcc.gov/ecfs/

Federal Communications Commission
FCC Wireline Competition Bureau, Competition Policy Division
445 12th Street SW
Washington, DC 20554

RE: WC Docket No. 16-106

To Whom It May Concern:

This comment is submitted on behalf of the Email Sender and Provider Coalition ("ESPC") in response to the Federal Communications Commission's request for public comment to its Notice of Proposed Rulemaking ("NPRM") on how to apply the privacy requirements of the Communications Act to broadband Internet access service ("BIAS").[1] The ESPC appreciates this opportunity to comment on how the FCC's broadband privacy rules can support the entire email ecosystem.

The Email Sender and Provider Coalition is a cooperative group of industry leaders working to create solutions to the continued proliferation of spam and the emerging problem of legitimate email deliverability. ESPC's membership provides mail delivery services to an estimated 250,000 clients, representing the full breadth of the U.S. marketplace. The ESPC's mission is to advocate on behalf of email senders, providers, and other digital marketers operating globally in the online, mobile, and social media environments in favor of global laws and self-regulatory efforts that balance consumer protection and business innovation; to educate its membership on current and emerging business and legal developments affecting its membership; and to continue to develop and refine best practices that foster innovation, industry growth, and consumer trust.

The ESPC questions at the outset the Commission's legal authority to impose such a sweeping new privacy framework as proposed by the NPRM. The NPRM cites as legal authority Section 222 of the Communications Act, which instructs the FCC to protect both proprietary information and "customer proprietary network information" ("CPNI").[2] While proprietary information has historically been understood as referring to CPNI, the Commission has only recently begun to

[1] 81 Fed. Reg. 23360 (proposed April 20, 2016).
[2] ¶¶ 278-82, 81 Fed. Reg. 23396-97.

interpret each term as creating independent legal obligations,[3] and the NPRM finds new authority under Section 222(a) to impose a broader set of protections over customer information than that imposed on CPNI under Section 222(c).[4]

The NPRM further suggests authority can be found in Sections 201 and 202 of the Communications Act, which prohibit telecommunications carriers from engaging in unjust, unreasonable, or unreasonably discriminatory practices.[5] The FCC equates prohibitions against these types of practices with prohibitions against "unfair and deceptive" acts and practices under Section 5 of the FTC Act.[6] However, the FCC's proposed privacy framework presents none of the limitations that exist under the Federal Trade Commission's policy statements on deception or unfairness, and the ESPC respectfully requests that the FCC refrain from asserting additional regulatory authority based on such statutory language.[7]

The remainder of our comments discuss the need for members of the email ecosystem to share certain information in order to combat spam, improve the deliverability of email, and to otherwise manage the reputation of legitimate email senders. We address how provisions in the NPRM might negatively affect the ability of email service providers ("ESPs") that provide email marketing services to address email abuse, junk emails, and fraudulent phishing emails in circumstances where BIAS providers are offering email services.

I. Sharing Data to Address Spam and Other Unwanted Emails

Today, when consumers grow tired or frustrated by email messaging, they have three clear options: to unsubscribe; to block the message; or to mark the message as "spam." While legitimate email senders long have provided unsubscribe features, and while such mechanisms are required under the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM Act"),[8] frequently consumers have found it easier to mark unwanted

[3] Peter Swire, Comments to the FCC on Broadband Consumer Privacy 3 (Apr. 28, 2015), https://transition.fcc.gov/cgb/outreach/FCC-testimony-CPNI-broadband.pdf.

[4] ¶ 280, 81 Fed. Reg. 23397.

[5] ¶ 276, 81 Fed. Reg. 23397.

[6] *See* In re: Joint FCC/FTC Policy Statement for the Advertising of Dial-Around and Other Long-Distance Services to Consumers (Mar. 1, 2000), https://www.ftc.gov/system/files/documents/public_statements/297751/000301jpsdeceptoveads.pdf.

[7] *See* Swire, *supra* note 3. *See also* Coalition Letter to Senate Subcommittee on Privacy, Technology, and the Law (May 10, 2016), https://www.ustelecom.org/sites/default/files/documents/Subcomittee%20Privacy%20Letter%205.10.16.pdf (noting that the Federal Trade Commission's enforcement of unfair or deceptive privacy practices "is consistent with the FCC's privacy recommendations in the 2010 National Broadband Plan.").

[8] 15 U.S.C. § 7704(a)(5).

emails as spam rather that unsubscribe or otherwise manage their email preferences.[9] This information is received by the consumer's mailbox provider, which then takes action to limit additional unwanted messaging.

Email mailbox hosting services can be provided by Internet companies like Google, Yahoo, and Microsoft, but hosting services and email servers are also provided by Internet service providers or broadband Internet access services as defined by the Commission's 2015 Open Internet Order.[10] If BIAS providers that offer email services are limited in their ability to share information about messages that consumers consider to be spam, the entire email ecosystem could suffer, and email senders would not just lose a significant part of valuable insights into why their messages were unwanted, but also unknowingly continue to send email to consumers that is unwanted by such consumers. This disconnect of information would also put at risk their ability to comply with applicable laws inside and outside of the United States.

These insights are derived from complaint feedback loops, or feedback loops ("FBL"), which have become one of the industry's primary tools to address spam and unwanted email. FBLs involve multiple organizations in the email ecosystem: online mailbox providers like AOL;[11] Outlook;[12] and Yahoo[13] and BIAS providers like Comcast[14] use FBLs to provide feedback to ESPs and their customers – the original senders of an unwanted message. This feedback mechanism begins when mailbox providers receive consumer complaints by placing "report spam" buttons on their webmail interfaces, in their desktop clients, or via help desks. Once a consumer reports spam or otherwise notifies their mailbox provider about an unwanted email, a complaint is registered with the mailbox provider. Mailbox providers then rely on complaint rates to dictate the deliverability of email messages, and as consumers have become more comfortable with these reporting mechanisms, an FBL closes the proverbial loop by allowing user complaints to get back to the originator of the unwanted email.[15] This process allows ESPs

[9] Direct Marketing Association, DMA Insight: Consumer Email Tracking Study 17 (2015), http://dma.org.uk/uploads/56543b6e6d645-email-tracking-report-2015_56543b6e6d5b5.pdf.

[10] 47 CFR § 8.2(a); 2015 Open Internet Order ¶ 347. *See also* Comcast, What Are Internet Service Providers?, http://www.xfinity.com/resources/internet-service-providers.html (explaining that many ISPs "offer email mailbox hosting services and email servers to send, receive and store email. Many mailbox ISPs are also access providers.") (last visited May 25, 2016).

[11] AOL Postmaster, AOL Inc., https://postmaster.aol.com (last visited May 25, 2016).

[12] Postmaster Services for Senders and ISPs, Microsoft, https://mail.live.com/mail/services.aspx (last visited May 25, 2016).

[13] Complaint Feedback Loop Program, Yahoo Mail, https://help.yahoo.com/kb/SLN3438.html (last visited May 25, 2016).

[14] Comcast, Feedback Loop Request Form, http://feedback.comcast.net (last visited May 25, 2016).

[15] MESSAGING ANTI-ABUSE WORKING GROUP (MAAWG), COMPLAINT FEEDBACK LOOP BEST CURRENT PRACTICES 6 (April 2010), *available at* http://www.internetsociety.org/sites/default/files/MAAWG_Complaint_Feedback_Loop_BCP_2010-08_0.pdf.

to monitor their complaint rates and to take steps to ensure they maintain a positive reputation as a sender of commercial emails.

This process occurs automatically, relieving mailbox providers from any need to review and forward complaints manually. Only authorized ESPs have access to a mailbox provider's feedback loop reports, and they must apply for and come to an agreement with each mailbox provider from which they wish to collect and receive user complaints. Legitimate email senders go through an application process that generally requires the sender or ESP to provide each mailbox provider with their contact information and IP addresses from which they send commercial email, as well as a dedicated email address to receive complaints before participating in an individual FBL.[16]

Feedback loops come in a variety of different forms, but most reports are sent in "Abuse Reporting Format" or "ARF."[17] ARF messages generally contain both machine-readable metadata and plain text to facilitate readability by human viewers with language like "This is an email abuse report for an email message received from IP 10.11.12.13 on Fri, 13 May 2016 09:25:55 +0000."[18] Reports include general feedback type such as whether the message was flagged for being abusive, fraudulent, or containing some type of virus or malware. They also can provide the following information to ESPs:

- the email address of the complainer;
- IP addresses;
- email headers; and
- the full body of the original email message.[19]

In addition to FBLs, mailbox providers increasingly are implementing an unsubscribe function that is separate from either spam reporting tools or in-message unsubscribe links. For promotional emails with unsubscribe options, mailbox providers can provide prominent notice at the top of the email near the sender's name to allow consumers to unsubscribe without looking around at the bottom of the message or otherwise having to leave their mailbox. Upon being clicked by a user, the mailbox provider automatically sends a request to the ESP and sender to remove the user's email address from their listing. This feature is only available to trustworthy

[16] Henry Gutierrez, Return Path, What Is a Feedback Loop? (June 27, 2013), https://blog.returnpath.com/what-is-a-feedback-loop/.

[17] Feedback Loop Formats, Messaging, Malware and Mobile Anti-Abuse Working Group, https://www.m3aawg.org/fbl-resources (last visited May 25, 2016).

[18] J.D. Falk, Return Path, Abuse Reporting Format Demystified (Sept. 9, 2010), https://blog.returnpath.com/arf-demystified/.

[19] *Id.*

senders in order to keep spammers and phishers from abusing this mechanism to validate if an email address is real or not.[20]

The information provided by these mechanisms is essential to help ESPs and the brands they work with better respect consumer choice and manage their lists and their email message content going forward. This, in turn, allows email senders to minimize the flow of unwanted messages into mailboxes and to ensure that consumers are only receiving the messaging they want. A steady flow of complaint information is important to help ESPs unsubscribe consumers, and if this information cannot be easily shared, it raises the likelihood that consumers may flag more and more messaging as spam. The result of such a scenario is irritated consumers and limits placed by mailbox providers, forcing them to limit the deliverability of messaging that is relevant to other consumers.

Even more important, however, is that information sharing is necessary to address network security across the email ecosystem. ESPs regularly cooperate with mailbox providers and other Internet security organizations to receive feedback on their messaging and work to identify security problems from specific senders and spammers.[21] Though legitimate email senders have put in place policies to prevent abuse by spammers, ESPs still rely on information from BIAS providers in order to identify network compromises, including fraudulent accounts and compromised hosts that attempt to take advantage of an ESP's services.[22] Network security is not something that email senders can take lightly. While unwanted emails can be an annoyance to consumers, malicious spam can present significant security concerns. The majority of email sent each day continues to be such spam, inviting consumers to share sensitive information, send cash overseas, or download suspicious and potentially harmful software.[23] These messages clog the services provided by mailbox providers and BIAS providers alike, and they present challenges to Internet security and to protecting consumers from fraud.

[20] *See, e.g.*, Tom Sather, *Everything You Need To Know About Gmail's Auto-Unsubscribe*, MARKETING LAND (Mar. 4, 2014), http://marketingland.com/everything-need-know-gmails-auto-unsubscribe-75605.

[21] Why M3AAWG?, Messaging, Malware and Mobile Anti-Abuse Working Group, https://www.m3aawg.org/about-m3aawg (last visited May 25, 2016).

[22] MESSAGING ANTI-ABUSE WORKING GROUP (MAAWG), COMPLAINT FEEDBACK LOOP BEST CURRENT PRACTICES 11, *supra* note 15; *see also* Gutierrez, *supra* note 16.

[23] Securelist, Spam and Phishing in Q3 in 2015 (Nov. 12, 2015), https://securelist.com/analysis/quarterly-spam-reports/72724/spam-and-phishing-in-q3-2015/ (finding that the percentage of spam in global email traffic was approximately 54.19% in late 2015).

II. Information Sharing under the NPRM

The information being shared by mailbox providers with ESPs is considered to be customer proprietary information ("PI") under the NPRM.[24] The NPRM takes an expansive view of what information can be properly classified as either customer proprietary network information ("CPNI") or personally identifiable information ("PII"), and the proposal defines PII to include any information that is either linked or linkable to an individual, including email addresses and other online contact information, IP addresses, and other account numbers and online identifiers.[25]

A. Exceptions to Address Fraud, Abuse, and Unlawful Use of BIAS

The NPRM recognizes that Section 222(d) of the Communications Act allows BIAS providers to use, disclose, or permit access to CPNI without customer notice or approval to "protect the rights of property of the provider, or to protect users and other providers from fraudulent, abusive, or unlawful use of, or subscription to, broadband services."[26] Mailbox providers, including BIAS providers, currently provide significant amounts of email security data to organizations that track spam and cyber threats such as phishing, malware, and botnets.[27]

Organizations must also share information in order to identify and detect from where on a network abuse originates. Spammers and other abusive email senders routinely attempt to use URL shorteners and other types of obfuscation to hide the contents of spam, and they regularly sign up for trial accounts or otherwise take advantage of ESPs in order to leverage the reputation of responsible entities to attempt to transmit spam. Feedback reports and other information about malicious senders help legitimate ESPs to uncover specific information about how their services are being used, to identify any technical or content problems with their marketing practices, and to take action both to mitigate abusive spam and to ensure IP addresses controlled by the ESP are not barred or blacklisted.[28]

IP addresses that become associated with computers or networks linked to spamming or other abusive online activities, whether merely unwanted email or malware, can be placed onto DNS-based black hole lists ("DNSBL").[29] Mailbox providers can take advantage of these lists to

[24] § 64.2003, 81 Fed. Reg. 23407.

[25] ¶¶ 42-44, 81 Fed. Reg. 23365-66.

[26] § 64.7002 Customer approval requirements, 81 Fed. Reg. 23409.

[27] *See, e.g.*, About Spamhaus, https://www.spamhaus.org/organization/ (last visited May 25, 2016).

[28] An email blacklist is a real-time database that uses set criteria to determine if an IP is sending email that could be considered spam.

[29] Carly Brantz, SendGrid, What is an Email Blacklist? (Oct. 30, 2013), https://sendgrid.com/blog/email-blacklist/.

ensure messages coming from these IP addresses can be flagged and rejected, and ESPs and their customers subsequently rely on the information received from FBL reports in order to tailor their lists and messaging practices so as to avoid becoming blacklisted. For example, feedback reports allow ESPs to see any complaint that is associated within a sender's IP space, and this information can then be used by ESPs and their customers to identify IP addresses that have been compromised by malicious third parties, as well as potential botnets,[30] to manage their reputations as legitimate senders, and to research how spammers are incorporating malware and phishing exploits into messaging.

The ESPC supports the language in Section 64.7002(a)(3) of the proposed rule that consumer approval to use, disclose, or access customer PI by BIAS providers may be inferred in such circumstances, and believes this exception likely covers use of FBLs and other information sharing mechanisms to identify network compromises and fraudulent accounts. However, it is unclear to what extent unwanted email messages alone constitute an abusive use of broadband services, and whether this exception would cover long-existing use of information now classified as customer PI to better manage mailing lists and email frequency or content. Minimizing unwanted messaging and security threats should be interpreted as measures to protect users and BIAS providers from fraudulent, abusive, or unlawful activities. The ESPC strongly suggests that Section 64.7002(a)(3) of the final rule have a specific exemption for the use, disclosure, and access of customer PI by BIAS providers and ESPs as follows: (1) to minimize abusive and unwanted emails; and (2) to permit sharing information in order to investigate, research, and address abusive or insecure mailing practices.

B. Exceptions for De-Identified or "Not Reasonably Linkable" Data

The NPRM's multi-pronged proposal for use, disclosure, and access to aggregate customer PI is grounded in existing guidance from the Federal Trade Commission.[31] The proposal embraces the principle that information is not "reasonably linkable" to consumers, computers, or devices when: (1) a given data set is not reasonably identifiable; (2) the company publicly commits not to re-identify it; and (3) the company requires any downstream users of the data to keep it in de-identified form.[32]

[30] A bot is a type of network malware that allows an attacker to take over a computer generally without their owner's knowledge; bots are generally part of a network of computers – or botnet – that are set up to forward transmissions (including spam or viruses) to other computers on the Internet.

[31] ¶¶ 136-148, 81 Fed. Reg. 23380-81.

[32] FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 22 (Mar. 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

The ESPC strongly supports this existing de-identification framework and believes it should be adopted as stated in Section 64.7002(g) of the proposed rules. This framework will help to facilitate the sharing of aggregated complaint data by BIAS providers with ESPs and other members of the email ecosystem. While many mailbox providers send individual ARF complaints, aggregated statistics and reporting can also provide ESPs and senders with valuable insights into how their messaging is performing, and thus provide valuable information if changes are necessary. Mailbox providers can receive many thousands of complaints and reports of spam from users, and aggregated reports allow mailbox providers to send ESPs and senders a clear message: if they receive a report, their messaging presents a serious problem.[33]

C. An Opt-Out Framework to Address Unwanted Emails is Appropriate

Absent these exceptions, the NRPM proposes to require BIAS providers to obtain opt-in consent from customers before customer PI may be shared with third parties.[34] Sharing elements of customer PI as discussed above is an important tool to reduce unwanted emails, and the proposed opt-in framework would limit this tool. It is likely that the use of FBLs would be significantly curtailed by mailbox providers that are also BIAS providers subject to the FCC's jurisdiction. Customers will see more unwanted emails, as well as more emails that pose a security threat, as a result.

The NPRM seeks comment on whether an opt-out approval framework might be appropriate for some subset of BIAS providers' activities or disclosure of customer PI to third parties,[35] and the ESPC strongly recommends that the final rule not require consumer opt-in with respect to efforts to address abusive and unwanted emails, as well as emails that pose a security threat. When this sharing is initiated by a consumer's direct action to unsubscribe from or otherwise limit messaging, further use by and disclosure to ESPs is within consumers' reasonable expectations. Consumer expectations and respect for context are important privacy principles recognized by the White House Consumer Privacy Bill of Rights.[36] Personally identifiable information should always be used in ways that are consistent with the context in which consumers initially provided the data, and efforts by BIAS providers and others in the email ecosystem to reduce abusive, unwanted, and insecure emails is clearly consistent with how consumers expect their data to be used when they select a mailbox provider and take advantage of spam reporting and unsubscribe mechanisms.

---

[33] Clea Moore, Return Path, What Is Aggregate Complaint Data and How Should You Use It? (Dec. 11, 2014), https://blog.returnpath.com/what-is-aggregate-complaint-data-and-how-should-you-use-it/.

[34] § 64.7002(f).

[35] ¶ 115, 81 Fed. Reg. 23376-77.

[36] WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 15 (2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

The ESPC further notes that the NPRM recognizes the need to use and disclose telephone numbers without additional customer consent to help protect consumers from abusive, fraudulent, or unlawful robocalls. The FCC cites robocalls as a chief complaint from consumers and concludes that "[a]t best, robocalls represent an annoyance; at worst they can lead to abuse and fraud."[37] Similar logic applies to abusive, unwanted, and insecure email. Spam messages continue to be of significant concern to consumers,[38] and consumers expect all mailbox providers, including BIAS providers, to pursue solutions that could help protect consumers.

These activities work to directly benefit the consumer email experience, and neither consumers nor companies should be burdened to seek and obtain consent to engage in such sharing. The ESPC proposes that BIAS providers be permitted to share customer PI to facilitate better email blocking and filtering solutions by consumers and third parties. The final rule should also permit BIAS providers to share information with ESPs in order: (1) to keep their databases clean of subscribers who no longer want to receive the sender's mail; and (2) to maintain the security of the emails they send.

III. Reasonable Data Retention Periods

Finally, the NPRM seeks comment on whether rules should require BIAS providers and others to set reasonable retention limits for customer PI.[39] The ESPC supports efforts by its members to establish reasonable retention limits for personal information and security data alike, particularly when such data may be immediately accessible and not stored remotely on backup tape. However, rapidly evolving practices across the Internet caution against the imposition of a strict retention period for customer PI, particularly mailing information.

Moreover, email data may already be subject to different retention requirements across a variety of regulatory regimes. For example, the Securities and Exchange Commission has imposed a three-year retention period for records involving communications relating to a broker-dealer's business and an even longer retention period for certain other records.[40] Other rules and regulations impose differing retention periods depending upon the type of record and sensitivity of information. Subjecting BIAS providers to additional data retention requirements may not only be burdensome and conflict with established laws or best practices; it may also inadvertently limit the ability of BIAS providers to research and monitor emerging security

[37] ¶¶ 100-101, 81 Fed. Reg. 23374-75.

[38] The Federal Trade Commission's Consumer Sentinel Network reports upwards of 10,000 consumer complaints regarding unsolicited email each year. FTC, CONSUMER SENTINEL NETWORK DATA BOOK FOR JANUARY - DECEMBER 2015, Appendix B3: Consumer Sentinel Network Complaint Category Details (Feb. 2016), *available at* https://www.ftc.gov/reports/consumer-sentinel-network-data-book-january-december-2015.

[39] ¶ 207, 81 Fed. Reg. 23387.

[40] 17 CFR 240.17a-4.

incidents with respect to abusive, fraudulent, or insecure email messaging and share that information with ESPs to help them protect consumers.

***

The ESPC appreciates the opportunity to submit comments in this important proceeding. If you have any questions concerning these comments, or if we may otherwise be of assistance in connection with this matter, please do not hesitate to contact me at 202-663-6267.

Sincerely,

D. R. Freeman

D. Reed Freeman, Jr.
Outside Counsel
Email Sender & Provider Coalition

cc: ESPC Board of Directors