

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 Return Path, Inc. (“Return Path”) in response to the Federal Communication Commission’s (“Commission”) 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”). Return Path appreciates this opportunity to comment on how the FCC’s broadband privacy rules can support the entire email ecosystem.

Return Path is the world’s leading email data solutions provider. Every minute of every day, our clients and partners trust our data and insights to help them build closer, safer, and smarter relationships with their customers.

Through the Return Path Data Exchange, we’ve brought together the world’s most comprehensive sources of data from the email ecosystem. We partner with more than 70 providers of mailbox and security solutions, covering 2.5 billion inboxes—approximately 70% of the worldwide total. Also feeding into the Data Exchange platform is our consumer network of more than 2 million consumers, representing purchasers from 5,000 retailers around the world. This wealth of data enables us to offer solutions which not only reduce unwanted emails and provide brand protection against email based threats, but also deliver unparalleled insight into purchase behavior, brand affinity, and consumer behavior and preferences.

Return Path was founded in 1999. Headquartered in New York, we have offices in Denver, Sunnyvale, Austin, Indianapolis, Toronto, London, Paris, Munich, Hamburg, Sydney, and Sao Paulo.

Return Path 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”). While proprietary information has historically been understood as referring to CPNI, the Commission has only recently begun to interpret each term as creating independent legal obligations, 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).

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. The FCC equates prohibitions against these types of practices with prohibitions against “unfair and deceptive” acts and practices under Section 5 of the Federal Trade Commission Act. However, the FCC’s proposed privacy framework presents none of the limitations that exist under the Federal Trade Commission’s (“FTC”) policy statements on deception or unfairness, and Return Path cautions the FCC against asserting additional regulatory authority based on such statutory language.

The FCC’s NPRM is not consistent with the established approach of the FTC, and would result in a different and problematic regime for those who are already under the FTC regulatory power and many others U.S. government regulatory bodies addressing privacy already in the areas the FCC NPRM proposes. Both consumers and the industry benefit when one agency takes the lead on privacy regulation and enforcement. The FTC has a long history of addressing and enforcing privacy-related issues across industries.

Additionally, the FCC has not sufficiently analyzed the implications of its NPRM, but is now rushing to finalize its flawed proposal; in fact, it denied the industry’s request for a reasonable extension of time to properly evaluate and advise the FCC on the NPRM’s impact. The limited time for the creation of a robust record is all the more concerning when the FCC does not have the FTC’s long history of expertise on this issue. The FCC would benefit from allowing more time for public comments.

We believe the FCC is overreaching and lacks congressional authority to issue the proposed regulation. Congress directed the FCC to foster competition among telephone providers, and in that context to enforce rules to safeguard the proprietary data that such providers maintained through their services. The FCC does not have authority from Congress to establish new privacy restrictions in the very different area of online data collection.

Instead of Congress changing the authority of the FCC, it should instead set a uniform national breach notification and data security standard which gets at the heart of FCC’s concerns with consumers information being collected, stored, and used. The FCC has proposed to regulate breach notification in a way that is contrary to the existing state notification regimes as well as the proposals under consideration by Congress. This would cause compliance burdens for businesses and confusion for consumers. Congress should establish a uniform standard for breach notification and data security.

Specific concerns with the NPRM:

- The proposed consent standard is too restrictive. The FCC has proposed to restrict most uses and disclosures of such data with an “opt in” consent standard. Consumers have embraced today’s thriving Internet, which is fueled by responsible data practices governed by the existing regulatory framework. Where consumer choice is warranted, an opt-out or implied consent standard is the best way to recognize consumer privacy preferences with respect to these types of online data while allowing legitimate practices, including advertising, to continue.
- The current online ecosystem subsidizes online offerings that consumers value, promotes innovation, and grows the economy. There is no record of consumer harm that supports the FCC’s proposal for such restrictive regulations.
- The proposed broadening of CPNI to include IP addresses, domain names, and other generic transactional metadata should be dropped. We appreciate the Commission’s desire to protect consumers, and we believe leaving the definition of PII open will ultimately prove more successful.
 - IP addresses and domain name information are not always analogous to telephone numbers in the voice telephony context. Many BIAS customers are assigned a dynamic (“changing”) IP address when they connect to their provider. In these cases, each time a consumer’s computer (or router) is rebooted, the ISP dynamically assigns a new IP address to the networking device. While the BIAS provider will have a record of precisely which user was connected to an IP address at a specific point in time, any third party will not, unless they subpoena the BIAS provider for data.
 - NAT (network address translation) addresses can refer to one -- or thousands -- of users which sit behind the NATted IP. NATing allows a router to modify packets to allow for multiple devices to share a single public IP address, therefore saving on costs and the current exhaustion of IPv4 addresses. The main use of NAT is to limit the number of public IP addresses an organization or company must use, for both economy and security purposes. External servers and users cannot distinguish between multiple inside clients behind a NAT.
 - The current assignment methodologies of IPv6 addresses often result in one device being assigned a range of IP addresses, naturally making “tracking a single user” much more difficult.
 - IPv6 address assignment occurs by combining a device’s network address with the MAC address assigned to the device’s network interface. While this theoretically gives a globally unique address to a computer, mobile phone, or device, the engineers who created IPv6 were very concerned about end-user privacy. Via RFC 4941, they defined a standard whereby end-user devices can generate completely random, frequently changing, host addresses to replace a device’s fixed MAC address. While the change interval can be set to anything, most operating systems have it set at one day.
 - In mobile networks, a device’s IPv6 address may change far more often than once per day. As the device owner physically moves through the

due course of his/her day (ex: connecting to wifi networks, traveling from home to work), the end user will receive a new IPv6 address. Ergo, while an IPv6 address could be extremely targeting, the reality is it won't often be a reliable source for creating user profiles.

- The European Union folds IP address into their definition of PII. As Return Path works closely with E.U. based BIAS and mailbox providers through our global data exchange, we speak authoritatively when we say that the E.U. definition has severely limited European BIAS and mailbox provider ability to fight not only email spam, but other forms of fraud and abuse, such as new user registration fraud, messageboard/online community harassment, and account hacking.
- The proposal to include all email message bodies under the definition of PII should be reworked to include a measure of risk to the consumer. Broadly declaring all email bodies to be PII -- regardless of content -- will hurt industry efforts to curtail abuse.
 - 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 sender 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"), frequently consumers have found it easier to mark unwanted emails as spam rather than unsubscribe or otherwise manage their email preferences. These "report spam" events are received by the consumer's mailbox provider, which then takes action to limit additional unwanted messaging. If BIAS providers that offer email services are limited in their ability to share "report spam" events, the entire email ecosystem could suffer. Email senders may lose not just valuable insights into why their messages were unwanted, but also unknowingly continue to send email to said consumers. 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.
 - Return Path operates FBLs for many BIAS providers, online retailers, and email service providers (ESPs). Information sharing is necessary to not only address the issue of over-zealous (but legitimate) email marketers, but also to more quickly stop email spam and other network abuses.
- The FCC's proposal to regulate data retention practices should be dropped.
 - Existing contracts between BIAS providers and third parties already protect against third party data misuse. Many also explicitly define destruction and retention periods based on service relationship requirements (ex: reputation-based, and/or machine-learning based systems).
 - Other US agencies and self-governing bodies already provide principles and laws around data retention. Ex: FTC Staff Online Behavioral Advertising Principles, Direct Marketing Association's Self-Regulatory Practices, and SEC's broker-dealer communications requirements. Additional requirements by the FCC will cause industry confusion at best. At worst, it will cause large financial

burdens -- impeding technical investment -- while providing no additional consumer protection.

- Placing limits on BIAS data retention may limit BIAS providers' ability to research and monitor emerging security incidents, ultimately harming consumers.
- In March 2006, the EU enacted a Directive on Mandatory Retention of Communications Traffic Data, which requires Member States to require communications providers to retain communications data for a period of between 6 months and 2 years. However, on April 8, 2014, the European Court of Justice struck down the Data Retention Directive because it violated the fundamental right to privacy. According to the Court, the Directive imposed "a wide-ranging and particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data, without that interference being limited to what is strictly necessary." Given the state of our ongoing talks with the E.U. regarding the U.S. Privacy Shield, we strongly oppose adding language which would go against E.U. rulings.
- The NPRM process also seeks to comment on alternative approaches to defining PII. For example, instead of defining the term PII, what are the benefits and burdens of leaving that term undefined and simply providing guidance on what types of information qualify? What are the benefits and burdens any alternative approaches?
 - We at Return Path think that it is best to leave such a definition open and for the FCC to only provide guidance on such things as we feel there is no way to create and maintain an exhaustive list of everything that constitutes PII in today's ever changing world of technology.
 - We already know that the fast paced movement of tech outpaces regulatory changes on a regular basis. Case in point, the CAN-SPAM Act of 2003, signed into law by President George W. Bush establishes the United States' first national standards for the sending of commercial e-mail and requires the Federal Trade Commission (FTC) to enforce its provisions. However, we've only had one single "clarification" in 2008 and since then the FTC along with Congress have no plans to update it again. We are the only country in the world with comprehensive email regulations that is on the opt-out and does NOT regulate well the changes in communication technology such as social media today. What that has forced Return Path and the industry into doing is creating successful coalitions like the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) which works to promulgate best common practices documents. As an example, the M3AAWG Senders Committee developed a set of best common practices for electronic communications to support the M3AAWG mission of reducing messaging abuse. The goal of these practices is to promote and enhance the transparency of senders maintaining legitimate messaging so that both individual recipients and BIAS or mailbox providers are more easily able to distinguish legitimate messaging from messaging abuse. This has enabled mailbox providers to more effectively use their resources in the fight against messaging abuse and to better protect end-users. M3AAWG categorically states that

verifiably clear, conspicuous and informed opt-in subscriber consent is the best practice for messaging permission. These documents outline these and other best practices and can keep up with changing technology.

- The NPRM seeks comment on how the FCC should define and treat the content of customer communications and asking if some or all forms of content should also be understood as customer PII.
 - At Return Path we caution the FCC once again to be careful about classifications of data as continued from above. 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 sender 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”), frequently consumers have found it easier to mark unwanted emails as spam rather than unsubscribe or otherwise manage their email preferences. 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. 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 may lose not just valuable insights into why their messages were unwanted but also unknowingly continue to send email to consumers that is unwanted by such consumers. 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; Outlook; and Yahoo and BIAS providers like Comcast use FBLs to provide feedback to ESPs and their customers – the original senders of the unwanted message. The information provided by these mechanisms is essential to help ESPs and the brands they work with better 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. 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.

Return Path 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 us at 1-866-362-4577 or privacy@returnpath.com. We also welcome the need of the FCC to have experts come to any townhall, roundtable meeting, or testimony based needs on this particular proceeding.

Sincerely,
/s/ Dennis Dayman

Chief Privacy and Security Officer
Return Path, Inc.