

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of)	
)	
Protecting the Privacy of Customers of)	WC Docket No. 16-106
Broadband and Other Telecommunications)	
Services)	
)	

COMMENTS OF CLOUDMARK, INC.

Cloudmark, Inc. (“Cloudmark”) hereby submits its comments in response to the Notice of Proposed Rulemaking (“NPRM”) in the above-captioned proceeding.¹

Cloudmark is a provider of security software and services. Cloudmark protects more than 120 tier-one service providers, including Verizon, Swisscom, Comcast, Cox and NTT, as well as tens of thousands of enterprises. Cloudmark estimates that it safeguards 12 percent of the world’s inboxes and 20 percent of mobile accounts from wide-scale and targeted email threats.

Cloudmark’s software includes: (1) Cloudmark Security Platform, which is a Message Transfer Agent (MTA) designed for use as a high performance email firewall to protect Internet Service Provider email services from email cyber threats ; (2) Cloudmark Authority, which is an anti-spam, anti-phishing, and anti-virus message content filtering solution designed for deployment within service provider messaging environments, and employs unique message fingerprinting technology to deliver high filtering throughput and accuracy against messaging borne cyber threats; (3) Cloudmark Trident, which is a spear phishing protection solution that

¹ Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, *Notice of Proposed Rulemaking*, FCC 16-39, (rel. Apr. 20, 2016) (“*Notice or NPRM*”).

enables detection of spear phishing attempts within a customer's inbound email stream, and leverages a unique combination of behavioral learning algorithms, reputation information, and message context analysis to score messages, enabling proactive notification of spear phishing and social engineering attacks; (4) Cloudmark Sender Intelligence, which provides a data feed of intelligence on IP addresses that have been sending malicious email content; and (5) Cloudmark Insight, which is an API into Cloudmark's knowledge of malicious domains and IP addresses.

For one or more of the products listed above, Cloudmark uses the following CPNI (as currently defined in the NPRM) and/or PII (as defined in the NPRM) in order to thwart various cyber security threats, including spam, malware, phishing and spear-phishing attacks:

- Email message content (RFC5322) sent to spam traps² and end users that may include email addresses of sender and recipient, IP addresses of all mail servers handling the content, domain information of the sender and recipient, subject information, additional specific PII or CPNI carried in the headers or the body of the email message and the entire contents of the email message including all URLs and IP addresses.
- Email protocol information (RFC5321) such as connecting IP address, sender email address and recipient email addresses.
- Geolocation information that may be attributed to IP addresses contained in email messages.
- Queried domains and IP addresses, where the BIAS provider utilizes information services provided by Cloudmark.

This information is used to recognize and quarantine malicious emails from reaching the inboxes of customers of the BIAS provider, thus reducing the amount of resources needed by the BIAS provider for all email traffic involving its customers, and reducing the amount of spam,

² Spam traps are email accounts that exist only for the purposes of receiving unsolicited spam messages. These are also known as email honeypots.

malware, phishing and spear-phishing attacks that could be clicked on to release its malicious payload.

Our comments focus on three areas:

1. Statutory exceptions where providers may use, disclose or permit access to Customer PI, without customer notice or approval³;
2. Accountability for third party misuse of customer PI⁴; and
3. The proposed definition of CPNI⁵.

Statutory Exceptions Where Providers May Use, Disclose or Permit Access to Customer PI without Customer Notice or Approval

As stated in Paragraph 115 of the *Notice*, the Commission seeks comment on its proposal to adopt the same exceptions set forth in Section 222(d) of the Act in the broadband context. Our comments focus on Section 222(d)(2) of the Act, which states that “providers may use, disclose or permit access to CPNI, without customer notice or approval, to . . . (2) protect the rights or property of the provider, or to protect users and other providers from fraudulent, abusive, or unlawful use of, or subscription to, broadband services”

We strongly believe that this exception is appropriate in the broadband context and also agree with the Commissions’ proposal that this exception should be expanded to include all customer PI. As stated above, we routinely use CPNI and PII to protect the BIAS provider and its customers from various spam, malware and phishing attacks. If the BIAS provider needed consent from its customers to use this information for this purpose, it could severely lessen the

³ See, *Notice*, ¶¶ 115, 117.

⁴ See *Notice* ¶¶ 210-213

⁵ See *Notice*, ¶¶ 41-55.

effectiveness of our software and services if customers do not provide the requisite approval, thus harming both the BIAS provider (who may have to invest in more resources to handle the increased volume of spam emails going through its systems) and its customers (who will receive more spam, malware and phishing attacks as a result of the reduced amount of data being provided to us). In addition, we feel that requiring consent from its customers for this purpose would be an unnecessary task to perform, since it is in everyone's interest to reduce spam, malware and phishing attacks. Finally, we believe that using CPNI and PII for this use is within the customers' expectations, since they do not want to have excess spam, malware and phishing attacks to reach their mailbox and they would expect their BIAS provider to use reasonable means to prevent such attacks from reaching them.

In paragraph 117, the *Notice* proposes that Section 222(d)(2) will allow "BIAS providers to use or disclose CPNI whenever reasonably necessary to protect themselves or others from cyber security threats or vulnerabilities."

We again strongly concur with this proposal, and more specifically, we believe that our software and services fall or should fall within this proposal. As you know, over 90% of all email traffic is estimated to be spam. This, as well as malware and phishing attacks, are all major cyber security threats that result in fraud, data breaches and other cyber security issues. We feel that the language in the final regulation should be sufficiently broad to allow for future types of cyber-security threats to fall under this exception without constant revisions to the regulation, and therefore, do not believe it makes sense to list what cyber security threats are entitled to this exception. However, we believe a non-exhaustive list would be helpful to give guidance. In this non-exhaustive list, we believe that services to prevent spam, malware and phishing attacks should be among the services listed that would be entitled to this exception.

Accountability for Third Party Misuse of Customer PI

As a third party that provides cyber-security software and services for BIAS providers, we are very interested in how best to ensure that the security, confidentiality and integrity of customer PI is protected once a BIAS provider shares it with a third party that is out of a BIAS provider's immediate control.

While we concur with the need to ensure that the entities contracting with BIAS providers should safeguard the data they receive, we believe a less prescriptive approach would be sufficient. BIAS providers and third parties should determine appropriate contractual commitment based on the sensitivity of the customer PI shared between the parties.

Having a required list of specific contractual commitments will not be flexible enough. In the same realm, requiring that the third party adopt the same data security requirements required for BIAS providers also will not be flexible enough. In reality, the type of customer data being disclosed should dictate the level of security needed. After all, it would be overkill to enforce the same security standards to treat IP address information, on the one hand, and credit card and social security information, on the other hand, in the same way. By requiring all third parties to adopt the same data security requirements as the BIAS provider, or prescribing a list of specific contractual commitments that a third party must adhere to, the Commission may unnecessarily restrict the third party's ability to conduct business by not allowing such third party to use its reasonable judgment to allocate scarce security resources to protect more important customer PI in a more secure way, but allow less important customer PI to be treated in a still secure, but less stringent way. We believe the BIAS provider and the third party are best able to determine the appropriate level of security needed based on the actual customer PI

being provided to such third party, and therefore, believe that the FCC shouldn't dictate such methods and have them applied to all customer PI.

Proposed Definition of CPNI

Assuming that the exception in Paragraphs 115 and 117 are adopted and are interpreted to include the software and services provided by companies like Cloudmark, then we have no direct interest in the precise definition of CPNI. However, we do note the following:

1. Many types of CPNI (as the Commission proposes to define it) are available in application payload and other meta information that are generally available to third parties other than the BIAS providers. Therefore, we believe that any generally available CPNI should not be subject to the NPRM, as it would unfairly regulate BIAS providers but not regulate the other third parties with access to the same CPNI information. For example, consumer IP information is readily available to a service operator (such as Facebook or Google) whenever a direct connection is made to its server and this service operator may associate it with an individual; however they will not be restricted in using this CPNI in the same way as the BIAS provider. In another example, a mailbox provider (such as Yahoo or Hotmail) will have access to all information contained in email protocols and content, which typically includes most of the CPNI defined in this NPRM, but will not be subject to the restrictions detailed in this NPRM. Instead, at most, the NPRM should only regulate customer PI that the BIAS provider knows solely by virtue of the BIAS relationship between such customer and the BIAS provider. For example, Cloudmark would agree that the dynamic IP address that has been

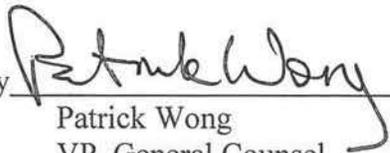
allocated to the consumer during the allocation window, which is provisioned by the BIAS provider and associated with the consumer, could be regulated by this NPRM, since this information is not generally known by anyone other than the BIAS provider.

2. The definition of CPNI may be better suited to be defined based on a well-understood network model such as the Open Systems Interconnection model (OSI model). For example, limiting the information based on various OSI model layers would more clearly delineate the boundaries since such network models are clearly understood by technical professionals. Information that is not carried in network protocols (e.g. geolocation information) would therefore not be considered CPNI. Additionally, specific network protocols that are covered by the NPRM should be specified, since the underlying assumption of the NPRM is that it is based on a TCP/IP network.
3. The definitions of elements considered CPNI are extremely general and therefore overlook specific implications of classifying the information as CPNI. Taken as a generality, this will impede a BIAS provider from operating the services based on this information. For example, geolocation information down to the square foot may be considered customer PII, but less specific geolocation to a state or country should not. The issue with being overly generic is that it affects every use case of that information.

Thank you very much for your time and attention. If you have any questions on these comments, please let us know.

Respectfully submitted,

CLOUDMARK, INC.

By  _____

Patrick Wong
VP, General Counsel
of

CLOUDMARK, INC.
128 King Street, Second Floor
San Francisco, California
(415) 946-3800

May 26, 2016