NPAC US Permitted Use Clarifications

Introduction

This document has been updated to provide details and clarifications on the Permitted Use of NPAC User Data for Service Providers and companies applying to become Providers of Telecommunications Related Services (PTRS) to assist in determining whether their proposed service aligns with the Permitted Uses. It is revised as of June 2020.

NPAC User Data is restricted and made available to qualified entities for Permitted Uses only. NPAC User Data or Derived Data from NPAC User Data can be used by authorized Service Providers (including Contracted Network Users of Service Providers), and PTRS for routing, rating, billing and network maintenance on behalf of Service Providers. Under other Ancillary Services Agreements, other entities may qualify to use specific elements of NPAC User Data for specific purposes, including law enforcement investigations, TCPA compliance, assessing risk and mitigating fraud. The focus of this document is on Permitted Uses for Service Providers and PTRS.

Permitted Uses are defined here for Service Providers (including their Contracted Network Users*) and PTRS who have a need to gain access to NPAC User Data in order to perform or facilitate network maintenance or the routing, rating, or billing of calls in connection with providing telecommunications services. Further, that NPAC User Data is required because these activities are impacted by porting or pooling. A limitation is imposed that the use of NPAC User Data cannot involve “commercial exploitation". There are numerous cases where NPAC User Data may be desired for other use cases such as risk assessment, fraud mitigation, TCPA compliance or Law Enforcement. These use cases may be permitted to qualified applicants via an Ancillary Service to the NPAC/SMS, however they are not permitted as a Provider of Telecommunications Related Services. Some specific examples of these applications are outlined below.

The following definitions are useful in understanding NPAC User Data and associated Permitted Uses for Service Providers and PTRS.

"Calls"

The term “calls” refers to the transmission of information (e.g., video, pictures, audio [voice, music], messages, text, data, or combinations of these) by use of a telephone number (NPA-NXX-XXXX), which may include the transmission of signaling messages or the transmission of provisioning data associated with information sessions, subscribers, and network equipment and devices (e.g., discovery, parameter negotiation, establishment, connection, maintenance, disconnection, presence, location, authentication, billing, and usage). Internet addresses and naming protocols (URLs, URIs, IP addresses, etc.) for the NUE Process are considered call routing information, so long as these items are associated with a telephone number.

Commercial Exploitation

The phrase “commercial exploitation of User Data” means the use of User Data for the sole, exclusive or principal purpose of, or having a material purpose of, marketing

telecommunications services to end users and consumers of telecommunications services or identifying those end users and consumers of telecommunications services and obtaining or retaining them as customers, provided, however, that access to the NPAC/SMS and use of User Data shall not constitute “commercial exploitation of User Data” merely because a charge or fee is associated with a service that uses or discloses User Data or because an economic benefit is derived from the provision of such service.

Contracted Network User

A Contracted Network User (CNU) is a Third Party that is a party to a written agreement with a User governing the terms and conditions of the Third Party’s use or sharing of, or access to, the User’s communications network. Note that this only applies to Service Providers. PTRS Users are not permitted to have Contracted Network Users. Amendments 21 and 21R to the LNPA Master Services Agreement provide further detail related to the Contracted Network User, and will be made available to a Service Provider or PTRS applicant once their NPAC New User Application has been approved.

Derived Data

Data derived, translated, or transformed from User Data (even if the original User Data is no longer present or imbedded in the resulting derived, translated, or transformed data) can only be distributed to recipients that have either a User Agreement or a PTRS User Agreement then in effect.

“For the Purpose of"

The phrase “for the purpose of” before the phrase "performance of network maintenance or the routing, rating, or billing of calls in connection with the provision of telecommunications services” is not limited to the case where the Applicant or User itself performs the network maintenance, routing, rating, or billing services, but rather also includes the case where the intended use of User Data is for the purpose of facilitating these activities performed by another party.

"Impacted by Porting or Pooling"

The phrase “impacted by porting or pooling” means that an activity cannot be performed satisfactorily without the use of User Data. For example, without the introduction of number portability or pooling, the identity of the Service Provider ("SP") serving a telephone number could be determined reliably using just the publicly available information about that telephone number’s NPA-NXX code. In a number portability or pooling environment, however, the use of User Data is required to reliably identify the Service Provider (and network and switch) serving the telephone number.

Limitation on Provision of User Data

A User may provide User Data to a third party only if that third party also is a User or PTRS User.

"Network Maintenance"

Network Maintenance - The phrase “network...maintenance in connection with providing telecommunications services” means any activity or process undertaken to ensure that operational, administrative, compliance, repair, and other functions of the User, including without limitation those concerning systems, databases used for telecommunications purposes, or networks, can be performed in an efficient, timely, or accurate manner.

Permitted Uses

The following definitions apply for purposes of determining whether an alleged need to access any part of the NPAC/SMS and intended use of User Data is a Permitted Use.

User Data may be used only for the purpose of performance of network maintenance or the routing, rating, or billing of calls in connection with the provision of telecommunications services, and then only where the network maintenance, rating, routing, or billing activity is impacted by porting or pooling.

An entity may obtain access to User Data merely to relay such User Data to Users, provided that such relay is accomplished through authorized methods (e.g., LSMS, etc.). The entity providing this relay of User Data is responsible only to assure that the recipients of the relayed User Data are themselves Users. Similarly, an entity may obtain access to the NPAC/SMS merely to relay User Data from Users to the NPAC/SMS, provided that such relay is accomplished through authorized methods (e.g., SOA, LTI, etc.). In both cases, the entity performing a relay of User Data between the NPAC/SMS and Users is a “Permitted Use” and deemed to be a PTRS Service or Administrator PTRS User Service, as applicable. In the course of these relay functions, the NPAC/SMS may return incidental User Data (e.g., NPAC/SMS notifications, audit request responses, etc.); the receipt of incidental User Data is not subject to the “Permitted Use” requirement."

Provider of Telecommunications Related Services (PTRS)

A PTRS is defined as a provider of telecommunications related services determined to have a need to access the NPAC/SMS and/or User Data, such as to route calls, bill calls or rate calls, or to perform network maintenance in connection with providing or facilitating the provision of telecommunications services. This category includes the Class 2 Interconnected VoIP provider, defined as an interconnected VoIP provider that partners with a facilities-based PSTN Service Provider to obtain NANPA numbering resources and connectivity to the PSTN via the Service Provider partner's PSTN switch, and which is not eligible to obtain NANPA numbering resources directly from the NANPA and the PA. This category also includes the Class 3 Interconnected VoIP provider, defined as a non-facilities-based reseller of interconnected VoIP services that uses the number resources and facilities of a Class 1 or Class 2 Interconnected VoIP provider (analogous to the "traditional" PSTN reseller). This category also includes Service Bureau’s that perform porting work on behalf of a Service Provider (SP).

"Routing, Rating or Billing"

- Routing - The phrase “routing of calls” means the transporting of calls.
- Rating - The phrase “rating of calls" means determining the applicable charge for calls.
- Billing - The phrase “billing of calls" means rendering a bill for calls.

Service Provider

The term “Service Provider” includes any entity to which PSTN numbering resources are assigned by the NANPA or the national Pooling Administrator. Telecommunications Service Providers (TSPs) are those entities that can own NPAC/SMS records and thus can create, modify, and delete these NPAC/SMS records. For example, a stand-alone VoIP provider (Class 1) is a TSP since it has agreed with the FCC to be bound by LNP rules and is allowed to receive assignments of NANP resources from the NANPA and the PA.

"Telecommunications-Related Services"

A Telecommunications-Related Service is a service that facilitates, or allows another, or allows another to allow another to rate, route, or bill calls, or perform network maintenance in connection with providing telecommunications services.

For purposes of the NUE Process, the term “telecommunications services” includes "telecommunications-related services."

User Data

Contractually, NPAC User Data is any Data provided by Users to the NPAC/SMS. Frequently requested User Data elements include:

- The current assigned Service Provider ID (SPID)
- The Service Provider type (wireless or wireline or VoIP)
- The Location Routing Number
- SS7 Destination Point Codes
- Service Type Alternative SPID (optional)
- Date and Time of Last Port

Examples of Permitted Uses

The following is a list of non-exclusive examples of Permitted Uses. These examples may be expanded as new uses are identified.

Examples of Network Maintenance Activities Representing Permitted Uses

Network maintenance is intended to be interpreted broadly, and includes, by way of illustration and not limitation, the following:

- Using the activation broadcast to determine when systems (such as LIDB, CNAM, Voice Mailbox, PSTN or other switching device, etc.) may be updated to reflect loss or gain of a customer.
- Using the User Data to determine current TSP to verify that a telephone number can be ported from a current TSP before programming a system to anticipate port-in of the number.
- Using the User Data to determine a TN’s current TSP to determine whether to take a trouble report or to comply with a legal request.
- Using the User Data to determine appropriate call routing translations.
- Using the User Data to administer a telephone number assignment system (pooling administration).
- Using the User Data to administer an inter-carrier billing system.
- Using the User Data to administer databases such as for monitoring, performance, accounting, security, etc.
- Using the User Data to administer databases used for network maintenance purposes.
- Service Bureaus providing porting services on behalf of a TSP.
- A 911 emergency database administrator that is responsible for verifying that the current TSP is shown for each telephone number contained in the database

Examples of Routing Activities Representing Permitted Uses

A network transporting a call to a ported number must determine the terminating network/switch serving the ported number, but is unable to rely on the dialed number.

A Medical Alerting Service provides text message appointment alerts to its customers. It disseminates the information under prior arrangement to its customers (e.g., opt-in). The Alerting Service does not use an aggregator to disseminate these alerts, but rather routes them directly to its customers' TSP gateways. The Alerting Service must know the identity of each customer's Service Provider to route these alerts. The Alerting Service cannot use User Data to determine whether the customer who has opted in still owns the phone number. In other words, the Alerting Service may use the User Data to route to the phone number but not necessarily to a designated individual.

A messaging aggregator provides text message routing on behalf of numerous clients, including enterprises, etc. The messaging aggregator may use User Data to route the message to the appropriate carrier on behalf of their clients. The messaging aggregator may not share User Data with their clients.

Messaging aggregator may also use User Data to distinguish between mobile and landline carriers for the purposes of routing of text messages. Neither the messaging aggregator nor their client may use the User Data to determine whether or not to send a message (e.g. to assess risk of whether a message is being routed to the person who opted in to receiving messages from a specific sender). Any analysis that is done with User Data to determine ***whether or not a call or message should be delivered*** is not considered to be a Permitted Use. This analysis may be addressed using the PortData Validate Service.

A VoIP provider must know the identity of the TSP serving the called number in order to determine whether there is an IP route to that provider or it must instead route the call through an associated PSTN gateway switch.

A VoIP provider must know the identity of TSPs serving ported numbers in a particular rate area in order to determine the economic benefits of establishing a presence in a PSTN switch serving that rate area or of establishing a direct IP traffic exchange with those TSPs.

Examples of Rating Activities Representing Permitted Uses

The cost for a call is dependent on which TSP is serving/owns the called party. The originating network must identify the provider serving the called number as calls terminating to a TN's owning carrier's network are generally better economically.

An Alerting Service provides text message alerts to its customers under prior arrangement to its customers (opt-in). The Service Providers' charges to their end-users for delivery of the alerts, and their charges to the source of the alerts for accepting the alerts, varies from one TSP to the next. The Alerting Service must know the identity of each of its customer's Service Providers in order to determine its prices.

Examples of Billing Activities Representing Permitted Uses

A reseller, or class 2/3 VoIP provider, obtaining number inventory from a CLEC partner, may need access to User Data in order to know the date on which a number has ported away ("activated") to know when its billing for services associated with the number should end.

An Alerting Service provides text message alerts to its customers. Service Providers may offer billing on behalf of the Alerting Service. The Alerting Service must know the identity of each of its customers' Service Providers in order to determine how to bill the Service Provider for alerts.

User Data cannot be used to determine the appropriate carrier for direct carrier billing, nor can it be used to assess fraud risk of transaction. Example: User Data was requested (e.g. recent porting history and current SPID) to 1) allow the applicant to query the proper mobile carrier 2) ensure that mobile number has not been compromised and then determine whether the direct carrier billing purchase can be approved.

Examples of Uses that are *not* Permitted as a PTRS

This list is not intended to be exhaustive. Some of these use cases may be permitted under an Ancillary Service that the Local Number Portability Administrator is authorized to offer (see https://numberportability.com/ for further information).

- Any support for entities such as financial institutions, insurance companies and merchants that need user authentication via One-time passwords during login or password reset process or as part of two-factor authentication
- Allowing the user to check with the appropriate carrier to assess risk as part of the analysis of whether or not to route calls
- Use of User Data to determine whether or not to route calls
- Use of Porting history derived from User Data to understand customer behavior or assess risk
- Any support for entities such as financial institutions, insurance companies and merchants that need to know the current Service Provider or porting history
- Use of recent porting history as an indicator of spam or Robocalling
- Use of recent porting history to assess the risk of a financial transaction before authorizing direct carrier billing
- Use of User Data for TCPA compliance
- Use of User Data for Law Enforcement Investigations