

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

In the Matter of)	
)	
Telecommunications Relay Service and)	CG Docket No. 03-123
Speech-to-Speech Services for)	
Individuals with Hearing and Speech)	
Disabilities)	
)	
Structure and Practices of the Video Relay)	CG Docket No. 10-51
Service Program)	

PETITION TO LIMIT ACCESS TO DATA IN THE iTRS NUMBERING DIRECTORY

Sorenson Communications, Inc. (“Sorenson”) respectfully petitions the Federal Communications Commission to direct Neustar, Inc. (“Neustar”) in its role as designated database administrator to limit iTRS providers’ access to certain numbering information stored in the centralized numbering database for Internet-based Telecommunications Relay Service (the “iTRS Numbering Directory”). At present, any iTRS provider can query the iTRS Numbering Directory to learn which ten-digit number or numbers are associated with a particular IP address. Because providers utilizing server-based routing can, and at least some do, associate a single IP address with many or all of their subscribers’ ten-digit numbers, this “reverse look-up” capability effectively makes a provider’s list of assigned numbers readily available to all other iTRS providers. While an iTRS provider has legitimate call routing-related reasons to determine whether there are any valid ten-digit numbers associated with a particular IP address, there is no legitimate technical or routing-related need for providers to learn specifically which numbers those are with respect to subscribers of other iTRS providers.

Accordingly, in order to preserve data privacy and eliminate the possibility of improper use of this existing functionality, the Commission should direct Neustar to eliminate the ability

of iTRS providers to query the iTRS Numbering Directory and receive complete ten-digit number reverse look-up information for subscribers that are not the querying provider's default users. Instead, iTRS providers should be permitted only to determine whether there are any valid ten-digit numbers associated with a given IP address for the sole purpose of completing calls, and not to obtain the number(s) themselves, except with respect to their own default users.

To the extent the Commission concludes that it cannot take action on this request without first addressing the permissibility of server-based routing for video relay service ("VRS"), it should conclude that 47 C.F.R. § 64.613(a) permits such offerings, which it can do pursuant to the pending Petition for Clarification or Waiver filed by Purple Communications, Inc. ("Purple") in June 2010. Server-based routing is essential to providing VRS service to mobile phones and enterprise settings with corporate firewalls, and enables unified communications. Rolling back the clock by interpreting the iTRS database rules to prohibit server-based routing would eviscerate functional equivalence.

I. THE COMMISSION CREATED THE iTRS NUMBERING DIRECTORY TO ALLOW FOR SEAMLESS CALL ROUTING WHILE ENSURING DATA SECURITY AND PRIVACY

In its June 2008 *iTRS Numbering Order*, the Commission addressed the need for a centralized database to enable routing of calls to and from iTRS users following the assignment of North American Numbering Plan ten-digit numbers.¹ The Commission called for the development of the iTRS Numbering Directory, recognizing that such a database would be necessary to enable "providers other than the default provider ... to obtain accurate routing

¹ See *Telecommunications Relay Services & Speech-to-Speech Services for Individuals with Hearing & Speech Disabilities*, Report and Order and Further Notice of Proposed Rulemaking, 23 FCC Rcd. 11,591, 11,610-20 ¶¶ 46-78 (2008) ("*iTRS Numbering Order*"); see also 47 C.F.R. § 64.601(a)(25) (defining TRS Numbering Directory); 47 C.F.R. § 64.613 (administration of the TRS Numbering Directory).

information for a particular user of Internet-based TRS.”² The Commission reasoned that access to the iTRS Numbering Directory should be restricted to iTRS providers—because they are the only entities with any legitimate need to access the data (for routing purposes), and because limiting access “will help to ensure the security of the central database and the privacy of the data contained therein.”³ After setting out general parameters regarding the need for data security and the protection of privacy, the Commission “defer[red] to the neutral third party administrator . . . to determine the most appropriate database architecture.”⁴ On September 9, 2008, the Commission awarded Neustar the contract to build and operate the iTRS Numbering Directory,⁵ and Neustar continues to operate it today.

II. TO ENSURE DATA SECURITY AND PRIVACY, THE COMMISSION SHOULD DIRECT NEUSTAR TO REPLACE THE iTRS NUMBERING DIRECTORY’S EXISTING REVERSE LOOK-UP FUNCTIONALITY

At present, the iTRS Numbering Directory makes a reverse look-up function available to providers through which any iTRS provider can query the iTRS Numbering Directory using a specific IP address and obtain a list of all of the ten-digit numbers associated with that address.⁶ With respect to IP addresses not associated with the querying provider’s own default users,

² *iTRS Numbering Order*, 23 FCC Rcd. at 11,616 ¶ 62; *see also* 47 C.F.R. § 64.611(c)(2)(ii)(B).

³ *iTRS Numbering Order*, 23 FCC Rcd. at 11,617 ¶ 67; *see also* 47 C.F.R. § 64.613(a)(3) (limiting access to providers and the Directory’s administrator).

⁴ *iTRS Numbering Order*, 23 FCC Rcd. at 11,617 ¶ 68.

⁵ *See Commission Awards Contract to Neustar Inc. to Build and Operate Centralized Database for Internet Based Telecommunications Relay Service Numbering System*, Public Notice, 23 FCC Rcd. 13,385, 13,385 (2008).

⁶ This problem is more acute due to the increasing importance of server-based routing, which enables such functionally equivalent features like call forwarding and unified communications services. Providers utilizing server-based routing may have thousands of numbers linked to a single IP address in the iTRS Directory. Thus, a single reverse look-up may reveal thousands of individuals’ ten-digit phone numbers.

Sorenson is not aware of any call routing-related or other legitimate reason why providers might need access to such information from the iTRS Numbering Directory. While a provider may legitimately need to learn whether there are *any* valid ten-digit numbers associated with a given IP address in order to complete calls, there is no reason the provider needs to know what those associated numbers are when those numbers are not associated with its own default users.

Making this information available jeopardizes data security and privacy in contravention of the Commission's stated goals when establishing the parameters iTRS Numbering Directory.⁷ For instance, a nefarious individual with access to the iTRS Numbering Directory could use the reverse look-up functionality to obtain a list of ten-digit numbers associated with another provider's customers, and he or she could use those numbers to populate "spoofed" caller IDs to create the impression that a particular provider's subscribers are making harassing calls, fraudulent calls, or are otherwise engaged in misconduct. Separately, the availability of ten-digit numbers associated with an IP address could allow providers to identify the numbers assigned to competitors' customers, and to target them with aggressive and unwanted marketing in an attempt to convince them to port.

Sorenson has discussed this issue with Neustar. Sorenson understands that Neustar is reluctant to make this change absent direction from the FCC to do so. Since there is no legitimate call routing-related or other technical reason to make this reverse look-up function available, and since its availability poses a risk to data security and customer privacy, Sorenson petitions to Commission to direct Neustar to disable it. In its place, Neustar should develop a feature that allows iTRS providers to query only whether there is one or more valid ten-digit

⁷ See *iTRS Numbering Order*, 23 FCC Rcd. at 11,616-17 ¶¶ 64, 67 (limiting authorized access to the database to iTRS providers "for the purpose of obtaining information from the database to complete calls" and "to ensure the security of the central database and the privacy of the data contained therein").

number(s) associated with a given IP address in order to complete calls, and not to obtain the number(s) themselves.

III. IF NECESSARY TO RESOLVE THE REVERSE LOOK-UP PROBLEM, THE FCC SHOULD CLARIFY THAT SERVER-BASED ROUTING IS PERMISSIBLE

To the extent the Commission finds it necessary to assess the permissibility of server-based routing before taking action the reverse look-up functionality, it should do so by taking action on Purple’s pending Petition for Clarification or Waiver.⁸ In its Petition, Purple “request[ed] the Commission to clarify whether server routing may be allowed in order to offer a call forwarding feature”; alternatively, Purple asked for a waiver of Section 64.613(a).⁹ Purple argued that the Commission had presumably not intended its rule to limit the ability of VRS providers to offer call forwarding and that “it would be discriminatory” to deny this feature to VRS users.¹⁰

Sorenson filed an ex parte letter on January 7, 2011, supporting Purple’s request and explaining that server-based routing is necessary to provide deaf consumers with functionally equivalent call-forwarding service: “Like hearing users of traditional voice communications, deaf VRS users require the ability to receive a call placed to a North American Numbering Plan number at different locations, including at home, at work, and on mobile devices—the so-called ‘follow-me’ feature that has been available to traditional voice consumers for a number of years.”¹¹ Server-based routing is also essential for VRS calls routed to PCs or mobile devices in

⁸ Petition for Clarification or Waiver of Purple Communications, Inc., CG Docket No. 10-51 (filed June 2, 2010).

⁹ *Id.* at 3.

¹⁰ *Id.* at 6.

¹¹ Letter from Christopher Wright, Counsel to Sorenson Communications, Inc., to Marlene H. Dortch, FCC Secretary, at 1, CG Docket Nos. 03-123 and 10-51, WC Docket No. 05-196 (filed Jan. 7, 2011) (“Wright Letter”).

public locations, as they depend on the dynamic IP address assignments that server-based routing enables.¹² As Sorenson noted in its ex parte letter, server-based routing greatly facilitates communications with VRS users located behind firewalls in the workplace or at home because the standards for NAT/firewall traversal developed by the ITU-T rely on an intermediate traversal server.¹³

Given the current industry movement toward SIP as a replacement for the H.323 protocol, the FCC should ensure that the design of the iTRS infrastructure follows SIP best practices, which would support server-based routing. The technical standard applicable to telephone number mapping (ENUM) for SIP specifies that the phone number in an ENUM database (the technology used to implement the iTRS Numbering Directory) should map to the “address of record” (that is, an identifier that corresponds to the individual user), rather than to a “contact address” (that is, the identifier associated with a particular device or endpoint).¹⁴ In fact, the standard warns that mapping to the device-specific contact address “would compromise the SIP capability negotiation and discovery process.”¹⁵

Relying on the user-specific “address of record”—not the device-specific “contact address”—is a core component of SIP communications. In a typical SIP-based communication, the calling party dials a number, and a proxy server associated with the calling party’s provider dips the relevant ENUM database to obtain the “address of record” associated with the dialed number. (The address of record takes the form of a fully-qualified SIP URI, like

¹² *See id.*

¹³ *See id.*

¹⁴ Peterson, J., Internet Engineering Task Force RFC #3764: “enumservice registration for Session Initiation Protocol (SIP) Addresses-of-Record” (April 2004), *available at* <http://www.ietf.org/rfc/rfc3764.txt>.

¹⁵ *Id.*

“sip:+1442079460148@sample.com”).) The proxy server then makes a Domain Name Server query (based on domain name, which is “sample.com” in this example), which returns back the “contact address” – which is the specific IP address for the proxy server where the user’s device is registered. The call is then routed from the calling provider’s proxy server to the terminating provider’s proxy server, which routes it to the called party’s device for completion. This *server-based* routing methodology is referred to as the SIP “trapezoid”,¹⁶ and is standard for SIP. The Commission should ensure that it permits this standard SIP functionality to function in the context of iTRS communications.

As Sorenson explained in its ex parte letter,¹⁷ the text of the Commission’s rules can be interpreted to permit server-based routing. In particular, Section 64.613(a)(2) of the Commission’s rules provides that “[f]or each record associated with a VRS user, the URI shall contain the user’s Internet Protocol (IP) address.” But a URI never literally “contains” anything; rather, it comprises a string of characters with a specific syntax pointing to a specific “location” on the Internet. A URI, in other words, must always be “resolved” to obtain a representation of the resource or “location” it identifies. Notably, Section 64.613(a)’s direction that a URI must “contain” a user’s IP address does not specify *how* the URI is to be resolved. Sorenson believes that it should be interpreted to include having the URI reference a *server* that can then resolve the appropriate IP “location” for the user. The most technologically and architecturally neutral reading of the rule is that it simply directs that the iTRS database must contain a URI that allows the provider handling the calling party’s call to route the call to the appropriate end user via that user’s IP address.

¹⁶ Rosenberg, J. and Schulzrinne, H., Internet Engineering Task Force RFC #3263: “Session Initiation Protocol (SIP): Locating SIP Servers” (June 2002), *available at* <http://www.ietf.org/rfc/rfc3263.txt>.

¹⁷ See Wright Letter at 3-4.

To the extent necessary for the Commission to reach the reverse look-up problem described above, Sorenson urges the Commission to clarify that this is the correct interpretation of Section 64.613(a).

Respectfully submitted,

Michael D. Maddix
Director of Government and
Regulatory Affairs
SORENSEN COMMUNICATIONS, INC.
4192 South Riverboat Road
Salt Lake City, UT 84123

/s/
John T. Nakahata
Charles Breckinridge
Renee Wentzel
WILTSHIRE & GRANNIS LLP
1200 Eighteenth Street, N.W.
Washington, D.C. 20036
T: (202) 730-1300
jnakahata@wiltshiregrannis.com

Counsel to Sorenson Communications, Inc.

February 16, 2012